

# Software Architecture

## *Foundations, Theory, and Practice*

PRIVATE DRAFT—NOT FOR DISTRIBUTION

Richard N. Taylor  
 Nenad Medvidovic  
 Eric M. Dashofy

Copyright © 2006-2007 Richard N. Taylor, Nenad Medvidovic, and Eric M. Dashofy. Do not distribute.

### TABLE OF CONTENTS

<b>1 THE BIG IDEA .....</b>	<b>19</b>
1.1 THE POWER OF ANALOGY: THE ARCHITECTURE OF BUILDINGS .....	20
1.1.1 <i>Limitations of the Analogy</i> .....	24
1.1.2 <i>So What's the Big Idea?</i> .....	26
1.2 THE POWER AND NECESSITY OF BIG IDEAS: THE ARCHITECTURE OF THE WEB .....	27
1.3 THE POWER OF ARCHITECTURE IN THE SMALL: ARCHITECTURE ON THE DESKTOP .....	33
1.4 THE POWER OF ARCHITECTURE IN BUSINESS: PRODUCTIVITY AND PRODUCT LINES .....	37
1.5 END MATTER .....	43
1.6 REVIEW QUESTIONS .....	44
1.7 EXERCISES .....	45
1.8 FURTHER READING .....	45
<b>2 ARCHITECTURES IN CONTEXT: THE REORIENTATION OF SOFTWARE ENGINEERING .....</b>	<b>47</b>
2.1 FUNDAMENTAL UNDERSTANDINGS .....	48
2.2 REQUIREMENTS .....	50
2.3 DESIGN .....	55
2.3.1 <i>Design techniques</i> .....	57
2.4 IMPLEMENTATION .....	60
2.4.1 <i>Implementation strategies</i> .....	61
2.5 ANALYSIS AND TESTING .....	65
2.6 EVOLUTION AND MAINTENANCE .....	68
2.7 PROCESSES .....	70
2.7.1 <i>The Turbine Model</i> .....	71
2.8 END MATTER .....	83
2.9 REVIEW QUESTIONS .....	85
2.10 EXERCISES .....	85
2.11 FURTHER READING .....	86
<b>3 BASIC CONCEPTS .....</b>	<b>88</b>
3.1 TERMINOLOGY .....	89
3.1.1 <i>Architecture</i> .....	89
3.1.2 <i>Component</i> .....	102
3.1.3 <i>Connector</i> .....	104
3.1.4 <i>Configuration</i> .....	106
3.1.5 <i>Architectural Style</i> .....	107
3.1.6 <i>Architectural Pattern</i> .....	108
3.2 MODELS .....	111
3.3 PROCESSES .....	112
3.4 STAKEHOLDERS .....	114
3.5 END MATTER .....	115
3.6 REVIEW QUESTIONS .....	115
3.7 EXERCISES .....	116
3.8 FURTHER READING .....	116
<b>4 DESIGNING ARCHITECTURES .....</b>	<b>118</b>
4.1 THE DESIGN PROCESS .....	120
4.2 ARCHITECTURAL CONCEPTION .....	122
4.2.1 <i>Fundamental Conceptual Tools</i> .....	123
4.2.2 <i>The Grand Tool: Refined Experience</i> .....	127
4.3 REFINED EXPERIENCE IN ACTION: STYLES AND ARCHITECTURAL PATTERNS .....	129
4.3.1 <i>Domain Specific Software Architectures</i> .....	131

4.3.2	Architectural Patterns.....	132
4.3.3	Introduction to Styles.....	138
4.3.4	Simple Styles.....	141
4.3.5	More Complex Styles.....	168
4.3.6	Discussion: Patterns and Styles.....	181
	Design Recovery.....	186
4.4	ARCHITECTURAL CONCEPTION IN ABSENCE OF EXPERIENCE: "UNPRECEDENTED" DESIGN.....	189
4.5	PUTTING IT ALL TOGETHER: DESIGN PROCESSES REVISITED.....	196
4.5.1	Insights from Requirements.....	197
4.5.2	Insights from Implementation.....	199
4.6	END MATTER.....	200
4.7	REVIEW QUESTIONS.....	201
4.8	EXERCISES.....	202
4.9	FURTHER READING.....	203
5	CONNECTORS.....	205
5.1	CONNECTORS IN ACTION – A MOTIVATING EXAMPLE.....	208
5.2	CONNECTOR FOUNDATIONS.....	210
5.3	CONNECTOR ROLES.....	212
5.4	CONNECTOR TYPES AND THEIR VARIATION DIMENSIONS.....	213
5.4.1	Procedure Call.....	214
5.4.2	Event.....	215
5.4.3	Data Access.....	216
5.4.4	Linkage.....	217
5.4.5	Stream.....	219
5.4.6	Arbitrator.....	220
5.4.7	Adaptor.....	221
5.4.8	Distributor.....	222
5.5	EXAMPLE CONNECTORS.....	223
5.5.1	Event-based Data Distribution Connectors.....	224
5.5.2	Grid-based Data Distribution Connectors.....	225
5.5.3	Client-Server-based Data Distribution Connectors.....	226
5.5.4	P2P-based Data Distribution Connectors.....	227
5.6	USING THE CONNECTOR FRAMEWORK.....	228
5.6.1	Selecting Appropriate Connectors.....	228
5.6.2	Detecting Mismatches.....	230
5.7	END MATTER.....	232
5.8	REVIEW QUESTIONS.....	234
5.9	EXERCISES.....	234
5.10	FURTHER READING.....	236
6	MODELING.....	237
6.1	MODELING CONCEPTS.....	238
6.1.1	Stakeholder-driven Modeling.....	238
6.1.2	Basic Architectural Concepts.....	240
6.1.3	Elements of the Architectural Style.....	241
6.1.4	Static and Dynamic Aspects.....	243
6.1.5	Functional and Non-Functional Aspects.....	244
6.2	AMBIGUITY, ACCURACY, AND PRECISION.....	245
6.3	COMPLEX MODELING: MIXED CONTENT AND MULTIPLE VIEWS.....	247
6.3.1	Views and Viewpoints.....	248
6.3.2	Consistency among Views.....	250
6.4	EVALUATING MODELING TECHNIQUES.....	252
6.5	SPECIFIC MODELING TECHNIQUES.....	253
6.5.1	General Techniques.....	253
6.5.2	Early Architecture Description Languages.....	265

6.5.3	Domain- and Style-Specific ADLs.....	279
6.5.4	Extensible ADLs.....	289
6.6	WHEN SYSTEMS BECOME TOO COMPLEX TO MODEL.....	305
6.7	END MATTER.....	306
6.8	REVIEW QUESTIONS.....	308
6.9	EXERCISES.....	308
6.10	FURTHER READING.....	309
7	VISUALIZATION.....	311
7.1	VISUALIZATION CONCEPTS.....	312
7.1.1	Canonical Visualizations.....	313
7.1.2	Textual Visualizations.....	314
7.1.3	Graphical Visualizations.....	315
7.1.4	Hybrid Visualizations.....	318
7.1.5	The Relationship between Visualizations and Views.....	319
7.2	EVALUATING VISUALIZATIONS.....	322
7.2.2	Constructing a Visualization.....	325
7.2.3	Coordinating Visualizations.....	329
7.2.4	Beyond Design: Using Visualization Dynamically.....	333
7.3	COMMON ISSUES IN VISUALIZATION.....	334
7.3.1	Same Symbol, Different Meaning.....	334
7.3.2	Differences without Meaning.....	335
7.3.3	Decorations without Meaning.....	336
7.3.4	Borrowed Symbol, Different Meaning.....	337
7.4	EVALUATING VISUALIZATION TECHNIQUES.....	337
7.5	TECHNIQUES.....	338
7.5.1	Textual Visualizations.....	338
7.5.2	PowerPoint-like.....	340
7.5.3	UML: The Unified Modeling Language.....	343
7.5.4	Rapide.....	348
7.5.5	The Labeled Transition State Analyzer (LTSA).....	350
7.5.6	xADL 2.0.....	354
7.6	END MATTER.....	358
7.7	REVIEW QUESTIONS.....	360
7.8	EXERCISES.....	361
7.9	FURTHER READING.....	361
8	ANALYSIS.....	363
8.1	ANALYSIS GOALS.....	367
8.1.1	Completeness.....	367
8.1.2	Consistency.....	368
8.1.3	Compatibility.....	375
8.1.4	Correctness.....	377
8.2	SCOPE OF ANALYSIS.....	377
8.2.1	Component- and Connector-Level Analysis.....	378
8.2.2	Subsystem- and System-Level Analysis.....	380
8.2.3	Data Exchanged in the System or Subsystem.....	382
8.2.4	Architectures at Different Abstraction Levels.....	383
8.2.5	Comparison of Two or More Architectures.....	385
8.3	ARCHITECTURAL CONCERN BEING ANALYZED.....	386
8.3.1	Structural Characteristics.....	386
8.4	LEVEL OF FORMALITY OF ARCHITECTURAL MODELS.....	387
8.5	TYPE OF ANALYSIS.....	388
8.6	LEVEL OF AUTOMATION.....	389
8.7	SYSTEM STAKEHOLDERS.....	391
8.8	ANALYSIS TECHNIQUES.....	393

8.8.1	<i>Inspections and Reviews</i>	394
8.8.2	<i>Model-Based Analysis</i>	399
8.8.3	<i>Simulation-Based Analysis</i>	407
8.9	END MATTER: TYING IT ALL TOGETHER	414
8.10	REVIEW QUESTIONS	415
8.11	EXERCISES	416
8.12	FURTHER READING	417
9	IMPLEMENTATION	419
9.1	CONCEPTS	420
9.1.1	<i>The Mapping Problem</i>	421
9.1.2	<i>Architecture Implementation Frameworks</i>	423
9.1.3	<i>Evaluating Frameworks</i>	424
9.1.4	<i>Middleware, Component Models, and Application Frameworks</i>	427
9.1.5	<i>Building a New Framework</i>	430
9.1.6	<i>Concurrency</i>	431
9.1.7	<i>Generative Technologies</i>	432
9.1.8	<i>Ensuring Architecture-to-Implementation Consistency</i>	434
9.2	EXISTING FRAMEWORKS	435
9.2.1	<i>Frameworks for the Pipe and Filter Architectural Style</i>	435
9.2.2	<i>Frameworks for the C2 Architectural Style</i>	438
9.3	EXAMPLES	447
9.3.1	<i>Implementing Lunar Lander in the Pipe-and-Filter Style using the java.io Framework</i>	447
9.3.2	<i>Implementing Lunar Lander in the C2 Style using the Lightweight C2 Framework</i>	454
9.4	END MATTER	466
9.5	REVIEW QUESTIONS	467
9.6	EXERCISES	468
9.7	FURTHER READING	468
10	DEPLOYMENT AND MOBILITY	470
10.1	OVERVIEW OF DEPLOYMENT AND MOBILITY CHALLENGES	474
10.2	SOFTWARE ARCHITECTURE AND DEPLOYMENT	477
10.2.1	<i>Basic Concepts</i>	477
10.2.2	<i>Deployment Activities</i>	478
10.2.3	<i>Tool support</i>	492
10.3	SOFTWARE ARCHITECTURE AND MOBILITY	495
10.3.1	<i>Basic Concepts</i>	495
10.3.2	<i>Mobility Paradigms</i>	496
10.3.3	<i>Challenges in Migrating Code</i>	497
10.4	END MATTER	498
10.5	REVIEW QUESTIONS	500
10.6	EXERCISES	500
10.7	FURTHER READING	502
11	APPLIED ARCHITECTURES AND STYLES	505
11.1	DISTRIBUTED AND NETWORKED ARCHITECTURES	506
11.1.1	<i>Limitations of the Distributed Systems Viewpoint</i>	507
11.2	ARCHITECTURES FOR NETWORK-BASED APPLICATIONS	508
11.2.1	<i>The REpresentational State Transfer Style (REST)</i>	509
11.2.2	<i>Commercial Internet-Scale Applications</i>	516
11.3	DECENTRALIZED ARCHITECTURES	518
11.3.1	<i>Shared Resource Computation: the Grid world</i>	519
11.3.2	<i>Peer-to-Peer Styles</i>	521
11.3.3	<i>Business-to-Business: Service-Oriented Architectures and "Web Services"</i>	528
11.3.4	<i>Summary Notes on Latency and Agency</i>	532
11.4	ARCHITECTURES FROM SPECIFIC DOMAINS	533

11.4.1	<i>Robotics</i>	533
11.4.2	<i>Wireless Sensor Networks</i>	540
11.5	END MATTER	542
11.6	REVIEW QUESTIONS	543
11.7	EXERCISES	544
11.8	FURTHER READING	545
12	DESIGNING FOR NON-FUNCTIONAL PROPERTIES	546
12.1	EFFICIENCY	549
12.1.1	<i>Software Components and Efficiency</i>	550
12.1.2	<i>Software Connectors and Efficiency</i>	553
12.1.3	<i>Architectural Configurations and Efficiency</i>	557
12.2	COMPLEXITY	560
12.2.1	<i>Software Components and Complexity</i>	561
12.2.2	<i>Software Connectors and Complexity</i>	565
12.2.3	<i>Architectural Configurations and Complexity</i>	568
12.3	SCALABILITY AND HETEROGENEITY	571
12.3.1	<i>Software Components and Scalability</i>	573
12.3.2	<i>Software Connectors and Scalability</i>	576
12.3.3	<i>Architectural Configurations and Scalability</i>	579
12.4	ADAPTABILITY	581
12.4.1	<i>Software Components and Adaptability</i>	582
12.4.2	<i>Software Connectors and Adaptability</i>	583
12.4.3	<i>Architectural Configurations and Adaptability</i>	586
12.5	DEPENDABILITY	587
12.5.1	<i>Software Components and Dependability</i>	589
12.5.2	<i>Software Connectors and Dependability</i>	591
12.5.3	<i>Architectural Configurations and Dependability</i>	592
12.6	END MATTER	593
12.7	REVIEW QUESTIONS	595
12.8	EXERCISES	595
12.9	FURTHER READING	596
13	SECURITY AND TRUST	598
13.1	SECURITY	600
13.2	DESIGN PRINCIPLES	605
13.3	ARCHITECTURAL ACCESS CONTROL	611
13.3.1	<i>Access Control Models</i>	611
13.3.2	<i>Connector-Centric Architectural Access Control</i>	613
13.4	TRUST MANAGEMENT	625
13.4.1	<i>Trust</i>	626
13.4.2	<i>Trust Model</i>	627
13.4.3	<i>Reputation-based Systems</i>	628
13.4.4	<i>Architectural Approach to Decentralized Trust Management</i>	632
13.5	END MATTER: TRADE-OFFS	642
13.6	REVIEW QUESTIONS	643
13.7	EXERCISES	644
13.8	FURTHER READING	644
14	ARCHITECTURAL ADAPTATION	645
14.1	CONCEPTS OF ARCHITECTURE-CENTRIC ADAPTATION	646
14.1.1	<i>Sources and Motivations for Change</i>	646
14.1.2	<i>Shearing Layers</i>	650
14.1.3	<i>Structural Elements Subject to Change</i>	654
14.1.4	<i>Change Agents and Context</i>	657
14.1.5	<i>Architecture: the Central Abstraction</i>	662

14.2 A CONCEPTUAL FRAMEWORK FOR ARCHITECTURAL ADAPTATION .....	663
14.3 TECHNIQUES FOR SUPPORTING ARCHITECTURE-CENTRIC CHANGE .....	666
14.3.1 Basic Techniques Corresponding to Activities of the Conceptual Framework .....	666
14.3.2 Architectures/Styles that Support Adaptation .....	677
14.3.3 The Special Problems of On-the-fly and Autonomous Adaptation .....	683
14.4 END MATTER .....	689
14.5 REVIEW QUESTIONS .....	690
14.6 EXERCISES .....	690
14.7 FURTHER READING .....	691
<b>15 DOMAIN-SPECIFIC SOFTWARE ENGINEERING .....</b>	<b>693</b>
15.1 DOMAIN-SPECIFIC SOFTWARE ENGINEERING IN A NUTSHELL .....	698
15.1.1 Similar Problems, Similar Solutions .....	699
15.1.2 Viewing DSSE through the Prism of Domain, Business, and Technology .....	701
15.2 DOMAIN-SPECIFIC SOFTWARE ARCHITECTURE .....	703
15.2.1 Domain Knowledge .....	704
15.2.2 Canonical Requirements .....	718
15.2.3 Canonical Solution Strategies—Reference Architectures .....	720
15.2.4 Product Lines and Architecture .....	723
15.2.5 Product-Line Concepts .....	724
15.2.6 Specifying the Architecture of a Product Line .....	726
15.2.7 Capturing Variations over Time .....	734
15.2.8 Using Product Lines as Tools for What-If Analysis .....	736
15.2.9 Implementing Product Lines .....	737
15.2.10 Unifying Product Architectures with Different Intellectual Heritage .....	740
15.2.11 Organizational Issues in Creating and Managing Product Lines .....	742
15.3 DSSAS, PRODUCT LINES, AND ARCHITECTURAL STYLES .....	743
15.4 DSSE EXAMPLES .....	744
15.4.1 Koala and Consumer Electronics .....	745
15.4.2 Software Defined Radios .....	748
15.5 END MATTER .....	754
15.6 REVIEW QUESTIONS .....	757
15.7 EXERCISES .....	758
15.8 FURTHER READING .....	759
<b>16 STANDARDS .....</b>	<b>760</b>
16.1.1 What are Standards? .....	761
16.1.2 Why Use Standards? .....	762
16.1.3 Drawbacks of Standards .....	764
16.1.4 When to Adopt .....	766
16.2 SPECIFIC STANDARDS .....	768
16.2.1 Conceptual Standards .....	768
16.2.2 Notational Standards .....	782
16.2.3 SysML .....	785
16.2.4 Standard Tools .....	789
16.2.5 Telelogic System Architect .....	792
16.3 PROCESS STANDARDS .....	793
16.3.1 Rational Unified Process .....	793
16.3.2 Model Driven Architecture .....	795
16.4 END MATTER .....	796
16.5 REVIEW QUESTIONS .....	798
16.6 EXERCISES .....	799
16.7 FURTHER READING .....	799
<b>17 PEOPLE, ROLES, AND TEAMS .....</b>	<b>801</b>
17.1 WHO ARE SOFTWARE ARCHITECTS? .....	803

17.1.1 Architect as a Software Designer .....	804
17.1.2 Architect as a Domain Expert .....	805
17.1.3 Architect as a Software Technologist .....	806
17.1.4 Architect as a Standards Compliance Expert .....	807
17.1.5 Architect as a Software Engineering Economist .....	808
17.1.6 Some Bad Habits .....	809
17.2 WHAT DO SOFTWARE ARCHITECTS DO? .....	811
17.2.1 Develop Project Strategy .....	811
17.2.2 Design Systems .....	812
17.2.3 Communicate with Stakeholders .....	812
17.2.4 Lead .....	813
17.3 HOW DO SOFTWARE ARCHITECTS WORK? .....	814
17.3.1 Balance of Skills .....	814
17.3.2 Allegiance to the Project .....	815
17.3.3 Allegiance to the Organization .....	816
17.3.4 Duration of Involvement .....	818
17.3.5 Team Structure .....	818
17.4 HOW DO SOFTWARE ARCHITECTS RELATE TO OTHER STAKEHOLDERS? .....	819
17.4.1 Architects and Engineers .....	820
17.4.2 Architects and Managers .....	821
17.4.3 Other Stakeholders .....	822
17.5 REMAINING CHALLENGES .....	823
17.6 END MATTER .....	824
17.7 REVIEW QUESTIONS .....	825
17.8 FURTHER READING .....	825
<b>18 END MATTER .....</b>	<b>827</b>
18.1 BIBLIOGRAPHY .....	827

## P R E F A C E

### Preface

Software architecture is the centerpiece of modern system development. The goal of architecture-centric development is the effective, efficient, competitive development of software *products*. The activities of development are anchored in the architecture. The goal for this text is to provide both student and professional a comprehensive treatment of architecture-centric development, instructing in how to develop products and serving as a reference for the panoply of techniques, modeling notations, standards, and methods comprising the approach.

With such an ambitious goal, the text is extensive and may be approached in different ways. In this preface we guide the reader in the use of the book. Hence we briefly present here:

- The general view of software architecture taken by the book
- The scope of the book
- A very short summary of each chapter
- The intended audiences
- Our assumptions regarding the technical maturity/background for professionals and students who are the users of the book
- Thoughts regarding selection of materials for use in the classroom, and by professionals, including:
  - Systems engineers
  - Software architects
  - Managers of software systems development
- How instruction in the material may be supported by tools

### Software Architecture

The text adopts a particular definition of software architecture: the set of principal design decisions governing a system. This definition is broad and stakeholder-centric. Nonetheless a decidedly technical view of software architecture pervades the book. We believe that software architecture must help developers create real implemented systems. Software architecture without a tie to implementation, deployment, and

long-term adaptation misses its potential by a wide mark and risks being irrelevant busy-work; tolerated perhaps, but not treasured.

The comprehensive character of software architecture as presented in the text makes it, in our estimation, the central focus of software engineering. The text attempts to show architecture's critical role in software engineering, yet the text does not attempt to be a general software engineering reference. There are, for example, many important parts of software engineering not treated at all, such as source code testing strategies, general project management; and development environments.

### The Scope of the Book

This book is characterized by breadth. Rather than focus on one method, notation, tool, or process, the book attempts to widely survey software development from an architectural perspective, putting many of these elements in context, comparing and contrasting them with one another. A reader should expect to gain a broad appreciation for the role of software architecture across the wide variety of activities that characterize the development of large, software-intensive systems.

The text is not a cookbook, nor is it a collection of canned solutions to a few specific problems. It does not advocate a single approach, nor is it a manual or "advertisement" for one—even the authors' own. Our assumption is that readers seek fundamental insights and knowledge to supplement their own experience. Hence, some thought will be required to apply the techniques and approaches described herein.

### Audiences

The book attempts to address the needs of several audiences.

The *professional* audience is supported with, for example, comprehensive treatment of the major modeling techniques, architectural description standards, and they way they are directly tied to the implementation of software products. Our perspective is not confined to some presumed ivory tower: the standards and notations include commercial, government, and research products. The text also attempts to provide, in the majority of chapters, specific guidance on how to achieve various goals, such as how to design to achieve specific system properties. References and examples draw from a wide range of industrial experience. Professionals should expect to encounter realistic and frank assessments of the techniques, notations, and tools that they are already familiar with, while also being exposed to projects and approaches that provide valuable insights but are nonetheless not well-known in practitioners' circles.

The *student* audience is supported with a presentation that is comprehensive, making relatively few assumptions about background knowledge and experience. We do assume that the student is generally familiar with the most basic elements of software engineering and programming. The order of the text and the way the material is presented makes the student the primary audience of the book – the other audiences will pick and choose material from various parts of the text.

The *systems engineer* will find that this book's perspective, while still focused on software, has implications that are quite a bit broader. Insights in this book will enable better understanding of the unique issues involved in the development of large *software* systems. Many of the insights, however, are applicable in *systems* development in general. Insights, notations, and methods from the systems engineering and systems architecture community are not ignored, and this book explores overlap between systems and software engineering throughout.

The systems and software development *manager* will find substantial material here that addresses the way in which architecture-centric development can shape and improve processes and organizations, especially with regard to the development of product families.

## Chapter Summaries

### Chapter 1: The Big Idea

The chapter introduces software architecture through discussion of three primary examples of its application: in the very large (the architecture of the World Wide Web), in the very small (pipe and filter on the desktop), and in the product/in the many (the Philips/Koala architecture for consumer electronics).

### Chapter 2: Architectures in Context: The Reorientation of Software Engineering

The role of software architecture in the major activities of software engineering is explored, including application conception, design, implementation, and analysis. An architecture-centric perspective on development is presented.

### Chapter 3: Basic Concepts

Definitions of the key terms and concepts are presented. The definitions build from the examples in the preceding chapters and form the foundation for the subsequent chapters.

### Chapter 4: Designing Architectures

The concepts of the preceding chapters are made productive in this one. This chapter presents, at length, techniques and approaches for designing applications from an architecture-centric perspective. The central focus is

on the ways in which refined experience may be used to guide new developments.

### Chapter 5: Connectors

Connectors play a distinguished role in architecture-centric development. They also are, perhaps, the most unfamiliar concept to those unskilled in the art of system design. This chapter reveals the breadth and depth of the concept, and includes an extensive guide to the numerous techniques available.

### Chapter 6: Modeling

This chapter surveys an extensive range of modeling notations used for capturing the design decisions that make up an architecture. Notations from research and practice are examined, and the distinctive aspects of each notation are called out. A consistent running example application is used throughout the chapter to demonstrate each notation.

### Chapter 7: Visualization

This chapter draws a distinction between how architectures are modeled—the syntax and semantics of how design decisions are documented—from how they are visualized. Visualization encompasses both depiction—how design decisions are presented—and interaction—the ‘user interface’ through which stakeholders interact with those depictions. Various visualization approaches are surveyed and compared, along with techniques for constructing and integrating new visualizations.

### Chapter 8: Analysis

One of the primary benefits of software architecture is that it can enable early assessment of a given system, before significant resources are invested in the system's implementation and deployment. This chapter provides a broad overview of the various analysis techniques that can be applied at the architectural level, their strengths, and limitations.

### Chapter 9: Implementation

This chapter describes the mapping problem of moving from architectural design decisions to implementation artifacts. Special attention is paid to the use of *architecture implementation frameworks*, special-purpose middleware that bridges the gap between architectural styles and existing platform services. Two complete implemented applications in alternative frameworks are presented with commentary.

### Chapter 10: Deployment and Mobility

This chapter addresses deployment and mobility, two related topics that have become very important in contemporary distributed, embedded, and pervasive systems. The objective of the chapter is not to provide a complete treatment of these two topics, but rather to isolate and focus on their characteristics from an explicit software architectural perspective.

### **Chapter 11: Applied Architectures and Styles**

Several examples from “the practice” are explored, showing how various of the ideas in the preceding chapters have been applied to solve deep and commercially important problems. The architectures of the World Wide Web, Napster, Gnutella, Skype, BitTorrent, robotics systems, Google, and Akamai are all discussed. The pedagogical goal is showing how multiple simple architectural approaches can be combined effectively.

### **Chapter 12: Designing for Non-Functional Properties**

This chapter selects a set of non-functional properties that are frequently required of large and complex software systems: efficiency, complexity, scalability, adaptability, and dependability. The role of software architecture in achieving the desired level of each property is discussed, and many specific architectural design guidelines are provided and discussed.

### **Chapter 13: Security and Trust**

Architecture-based techniques are presented for coping with security and trust needs in application system design. After a general introduction to security issues attention is focused on architecture-based access control and reputation-based trust systems.

### **Chapter 14: Architectural Adaptation**

The theme of this chapter is use of an architectural model to guide long-term system adaptation. A comprehensive conceptual framework for adaptation is presented, followed by consideration of numerous specific techniques for effecting adaptation and for designing applications to be accommodating of post-release adaptation.

### **Chapter 15: Domain-Specific Software Engineering**

Architecture-centric development is perhaps most valuable when applied in the context of a specific domain, where reuse of hard-won engineering knowledge and principles can substantially reduce the amount of effort, cost, and risk involved in system development. This chapter surveys a variety of techniques for applying architecture-centric development within a domain, and ends with an extensive treatment of product-line architectures.

### **Chapter 16: Standards**

A practicing architect or system developer is faced with a panoply of *de facto* and *de jure* standards—IEEE 1471, UML, SysML, DoDAF, RM-ODP, and so on. The chapter opens with a discussion of standards, how they are created and evolved, and how they can add value to development efforts. The remainder of the chapter surveys the most influential standards and attempts to put them in perspective, identifying their strengths and weaknesses explicitly.

### **Chapter 17: People, Roles, and Teams**

An effective architect may need to possess many different skills, beyond just being a good software designer. An architect is an integral part of a larger organization, and may be one of several architects working on a project. The context within which software architects operate, and therefore their job description, can get quite complex. This chapter overviews the various roles software architects may play in a project and, more broadly, an organization.

## **Assumptions and Background**

Depending on the sections of the book used for reference or in class, the necessary background varies. As a whole, however, the book assumes familiarity with the basics of software development. This includes the core ideas of software development activities and processes, notions of requirements, design, programming, and analysis and testing. The level of maturity required is, in some sense, only what would be acquired in a single, quarter- or semester-long introduction to software development/engineering. Appreciation for the problems of large-scale development is very useful. Proficiency in any particular programming language, development environment, or modeling tool such as UML is not required.

Experience, or maturity of thought, is perhaps the most important background for appreciating several of the chapters. Security and trust issues, for instance, are most appreciated by those who have (unfortunately) fallen victim to insecure software or have been scammed in an on-line auction. Similarly, appreciating the discussion of deployment or product lines demands some maturity in understanding how commercial development and product-and-revenue focused businesses work. The implementation chapter, on the other hand, will be of most value to those with substantive training and experience in programming.

## **How the book can be used**

The text can be used as a reference for systems engineers, software architects, managers, and programmers. It is also designed to be used as a textbook in formal classroom settings, both at the undergraduate and graduate levels.

Chapters 1 to 5 present the critical concepts of software architecture. Chapter 5 also bridges to the next section, the nuts and bolts of applying the concepts, which encompasses Chapters 6 through 10. Chapters 11 through 17 treat associated issues: topics that may be critical in one development context, but not in another.

### **Classroom usage**

There is adequate material in the book for a year-long class at the Master's degree level. The presentation does not presuppose that this is the normative case however. The authors have used material from the book in several settings already, including a one-quarter long undergraduate class in software engineering, a one-quarter long graduate introduction to software engineering, and a one-semester long graduate class in software architecture.

Clearly material has to be chosen based upon the level of the instruction and the length of the class. Nonetheless a few comments are in order. The "concepts section" is essential to use of the book. The material in the subsequent chapters depends on these core concepts. How long it will take to cover those initial chapters, however, will vary significantly. The first chapter, for instance, will be a very quick read for those with experience. Similarly, Chapter 2 will be relatively quick for those with experience in software engineering, but will take a bit longer in an undergraduate class that has minimal prerequisites. Chapter 4 is a long chapter. Nonetheless it is one topic and a critical one: a comprehensive treatment of how to go about designing a system. This chapter may thus be a major focus over many class sessions, especially for those with little training or experience in design.

Selection of materials from Chapters 6 through 10 will depend upon the level of the class, the course objectives, and the length of the class. The authors' bias is to recommend a shallow-but-encompassing view of all these chapters over a deep treatment of, e.g., just one of them, but this is of course up to the instructor.

A key issue the instructor will have to deal with is use of the exercises. Each chapter has a number of exercises listed. Software architecture is not a topic like algebra where numerous simple questions can be posed and answers given "in the back of the book". Software architecture concerns itself with design, with complex systems, and with long-lived products. Hence it is difficult to pose exercises which fit nicely into the constraints of a modern college class. Many of the questions included in the text could easily become mini-projects. The instructor will thus have to provide guidance to the students regarding the level of detail expected in the answers. Assessing the answers will similarly require thought and discretion.

### **Usage by Professionals**

The authors have endeavored to include substantial material to make the book a superior reference for the professional. A theme running through

the entire book is software reuse and, more generally, reuse of corporate and domain knowledge. Similarly there is explicit reliance in the presented techniques for use of frameworks to help achieve rapid system implementation. A wide range of modeling notations are discussed, and a complete chapter on standards is included to provide a thoughtful basis upon which a project can choose a notation or approach. Similarly the discussion of designing for non-functional properties is targeted at providing proven techniques capable of addressing these difficult issues. The chapter on designing (Chapter 4) will similarly be useful as a reference to the professional. Without being a "handbook of field techniques" it nevertheless presents a wide range of architectural styles and design techniques, with the styles summarized individually and in a comparison table to aid the professional in choosing the right technique for the job at hand.

### **Tool Support**

Use of the book in class or by professionals in practice does not require the use of any particular tool or programming language. Clearly, however, the subject is designing and building applications – products – and that only happens effectively in the presence of good tools.

The professional may be constrained by choice of the modeling notation required in a particular development context. If AADL, for example, is mandated as the architecture description language for a project, then the die is cast.

For those contexts where external constraints do not dictate, the instructor or reader is encouraged to use technologies that not only help model an architecture, but build implementations based upon those models. If modeling alone is supported, then the value of a tool over a simple boxes-and-arrows drawing tool rests upon the value obtained from analyses that can be performed on the model. If building real products is the goal, then a tool suite that addresses the full range of developers' needs is required.

To this latter end we encourage the book's users to evaluate the ArchStudio toolsuite, as it has been developed for this purpose. The tool is free, is integrated with the Eclipse development environment, and has been used in the classroom and in industry. A community of developers and users has formed around this project, with dozens of projects around the world using and contributing. Further details can be found on the project's website: <http://www.isr.uci.edu/projects/archstudio/>

## A C K N O W L E D G M E N T S

### Acknowledgments

The authors wish to express their sincere appreciation for the large number of people who have been instrumental in bringing this text to fruition.

Hazel Asuncion was instrumental in the development of the various Lunar Lander examples and the domain model for the Lander. Girish Suryanarayana and Jie Ren were key contributors to the chapter on security and trust. Sam Malek and Marija Mikic-Rakic supplied several figures and a number of key insights in our discussions of deployment and mobility. Chris Mattmann provided the material for data-intensive connectors presented in Chapter 5. George Edwards provided the example approach used in illustrating scenario-driven analysis in Chapter 8. John Georgas provided essential material for the discussion of robotics architectures in Chapter 11.

Kari Nies was an especially helpful and careful reviewer of the entire manuscript. The students of UC Irvine's Fall 2006 graduate class in software engineering (Informatics 211) and USC's Spring 2007 graduate class in software architectures (CSci 578) were early reviewers and commentators on key parts of the manuscript; their help is gratefully acknowledged. Similarly, the helpful comments of Peyman Oriezy, Roy Fielding, Scott Hendrickson, Michael Gorlick, David Woollard, Roshanak Roshandel, Daniel Popescu, George Edwards, and Chris Mattmann were very much appreciated.

External reviewers have included Professors Geoge Heineman and Tony Wasserman, both of whom provided particularly helpful suggestions and recommendations. Professors André van der Hoek, Jeff Kramer, Hans van Vliet, and Alex Wolf also provided important guidance. Several anonymous reviewers also contributed key insights for the work, as did MIT Press's Robert Prior.

University College London deserves special thanks for hosting Taylor's sabbatical in 2005-06, during which time the manuscript was substantially developed. A wonderful flat in Hampstead helped too.

The support of the National Science Foundation through grants CNS-0438996, CCF-0430066, CCF-0524033, CCR-9985441, ITR-0312780, and CSR-0509539, The Boeing Company, Bosch, the Jet Propulsion Laboratory, and IBM is gratefully acknowledged.

**CHAPTER 1****1 The Big Idea**

The study of software architecture is the study of how software systems are designed and built. A system's architecture is the set of principal design decisions made during its development and any subsequent evolution. As a subject, architecture is the proper primary focus of software engineering, for the production of high-quality, successful products is dependent upon those principal decisions.

An architecture-centric approach to software development places an emphasis on *design* that pervades the activity from the very beginning. Design quality correlates well with software quality—it would be extremely unusual to find a high-quality software system with a poor design. The practice of architecture-centric development can also enable the creation of cost-effective families of software products which can dominate an application sector over an extended period of time. Good design practices can leverage the lessons of experience and devise strategies for effectively meeting a wide range of needs.

This chapter introduces the central ideas of software architecture. It does so by first exploring the analogy between the architecture of buildings and the architecture of software. Software architecture, and the power that comes from making it the centerpiece of system development, is then illustrated three ways. First, the architectural ideas underpinning the World-Wide Web are explored – software architecture “in the very large”. Second, the ideas are explored on the desktop – software architecture in the small. Third, the central role of architectures in enabling successful product families is explored, using consumer electronics as the application domain. We deliberately omit most technical details, seeking rather to instill a sense of “the big idea”.

- 1. The Big Idea
- 1.1 The Power of Analogy: The Architecture of Buildings
  - 1.1.1 Limitations of the Analogy
  - 1.1.2 So What's the Big Idea?
- 1.2 The Power and Necessity of Big Ideas: the Architecture of the Web

**Outline of Chapter 1**

- 1.3 The Power of Architecture in the Small: Architecture on the Desktop
- 1.4 The Power of Architecture in Business: Productivity and Product Lines
- 1.5 End Matter
- 1.6 Review Questions
- 1.7 Exercises
- 1.8 Further Reading

**1.1 The Power of Analogy: The Architecture of Buildings**

The discipline of architecture, that is, the design and construction of buildings, offers a rich base of concepts from which software architecture, and more generally, software engineering has drawn. The analogy between the design and construction of buildings and the design and construction of software is strong, and is readily apprehended, since we all have substantial experience in living in and around buildings and in seeing them built.

Software engineering typically uses this analogy to motivate the phases of the traditional software lifecycle. In a highly simplified and idealized conception of architecture, requirements for a building are collected, a design is created to satisfy those requirements, the design is refined to yield elaborate blueprints, construction based on the blueprints is contracted and performed, and the resulting structure is then occupied and used. So, notionally, in the software domain requirements are specified, a high-level design is created, detailed algorithms are developed based upon that design, code is written to implement the algorithms, and finally the system is deployed and used.

The idealized outline above of how buildings come to be is almost trivial, but offers several insights reflected in the software domain. For instance, the architectural process has as its focus the satisfaction of the future occupant's needs. It allows for specialization of labor: the designer of the structure need not be the contractor who performs the actual construction. The process has many intermediate points where plans and progress may be reviewed. Thus with the simplistic view of software development: specification of a system's requirements precedes its design; that design is created by specialists, not by the ultimate users of a system. Actual programming may be contracted out, even off-shored. Prototypes and mock-ups created at various points during development enable the customer to periodically assess whether the emerging system will indeed meet the identified needs.

A more than trivial consideration of architecture, however, reveals deeper insights. First and perhaps foremost is the very conception of a building having an architecture, where that architecture is a concept separate from, but inextricably linked to, the physical structure itself. A building's architecture, that is, its major elements, their composition, and arrangement, can be described, discussed, and compared with those of other buildings. The architecture that was in the mind of the architect early in the development process can be compared with the architecture of whatever physical structure emerged from the construction process. So too, as we will shortly describe, the principal design decisions characterizing a software application – i.e. its architecture – exist independently from, but linked to, the code which ostensibly implements that architecture.

In the first century A.D. the Roman author Marcus Vitruvius Pollio, best known as Vitruvius, produced a famous treatise on architecture, entitled *De Architectura*. This handbook contains numerous admonitions, opinions, and observations about architecture and architects that remain, two thousand years later, insightful and worth considering. He begins his treatise in a remarkable place, considering the practice and the theory of architecture. Both are necessary for the professional.

"Practice is the frequent and continued contemplation of the mode of executing any given work, or of the mere operation of the hands, for the conversion of the material in the best and readiest way. Theory is the result of that reasoning which demonstrates and explains that the material wrought has been so converted as to answer the end proposed." I, 1, 1.

Note that practice is not the mere "doing", but involves contemplation of what is done.

#### Practice AND Theory

A second insight is that properties of structures are induced by the design of their architectures. For instance, a medieval castle with high, thick walls and narrow or non-existent windows is designed that way so that it has excellent defensive properties (as long as attackers are armed only with swords and arrows). So too, as we will see, properties of software applications, such as resilience in the face of particular types of security attacks, are determined by the design of their architectures.

#### Strength, utility, and beauty: The qualities obtained from good architecture

"All these should possess strength, utility, and beauty. Strength arises from carrying down the foundations to a good solid bottom, and from making a proper choice of materials without parsimony. Utility arises from a judicious distribution of the parts, so that their purposes be duly answered, and that each have its proper situation. Beauty is produced by the pleasing appearance and good taste of the whole, and by the dimensions of all the parts being duly proportioned to each other."

Vitruvius I, 3, 2.

A third insight is the recognition of the distinctive role and character of an architect, the person responsible for the creation of the architecture. The discipline of architecture has long recognized that architects require very broad training. While competence in aspects of engineering is necessary, much more than that is required. A fine sense of aesthetics and a deep understanding of how people work, play, eat, and live are essential in creating buildings that are enjoyed, satisfy their occupants, and perform effectively over the seasons and through the years. So too, simple skill in programming is insufficient for the creation of complex software applications that people can effectively employ.

#### Qualifications of an Architect

"An architect should be ingenious, and apt in the acquisition of knowledge. Deficient in either of these qualities, he cannot be a perfect master. He should be a good writer, a skilful draftsman, versed in geometry and optics, expert at figures, acquainted with history, informed on the principles of natural and moral philosophy, somewhat of a musician, not ignorant of the sciences both of law and physic, nor of the motions, laws, and relations to each other, of the heavenly bodies."

Vitruvius, I, 1, 3.

A fourth insight is that process is not as important as architecture. This is not to say that process is unimportant. On the contrary, architects and construction companies clearly follow and depend upon standard processes to guide their daily activities and ensure that all aspects of the design and build activities are addressed. But there is never any question that the product – the architecture – is the focus. Simply following a standard process will not guarantee that a successful building will emerge, meeting the needs of its owners and occupants. The architects and engineers responsible for the structure must keep its design and qualities at the forefront; process is there to serve those ends, not to be an end in itself.

A fifth insight is that architecture has matured over the years into a discipline: a body of knowledge exists about how to create a wide range

of buildings to meet many types of needs. It is not simply a discipline of basic principles and generic development processes, however. If every building had to be designed from first principles and the properties of materials had to be rediscovered for each new project, then most of us would be wet and shivering with the sky for our roof. The discipline of architectural engineering has captured the experiences and lessons of previous generations so that the process of designing, for instance, a new suburban home is much like the process of designing a thousand other homes. This is not to say that the homes are identical; rather, within the broad concept of "suburban home" some basics are established and points of allowable variation are known. Where there is commonality between two homes, great efficiencies can be realized through reuse of knowledge, reuse of subsystem design, reuse of tools, and the benefits that come from standardized materials, parts, and sizes. While anyone who has ever endeavored to build a custom home would certainly dispute that the process is "efficient", compared to the activity of designing from a truly clean slate, the craft works very well.

One fundamental way in which the experiences and lessons from previous generations of architects and building-dwellers has been captured is summed up in the notion of *architectural styles* – an insight that has powerful application in the domain of software. The phrases "Roman villa", "Gothic cathedral", "ranch-style tract home", "Swiss chalet", and "New York skyscraper" each characterize types of buildings which have various features in common. Ranch-style tract homes, for instance, are single-storey residences with low roofs; Swiss chalets are usually 2-4 stories, traditionally made of timber, have steep roofs, and large sheltered balconies. New York skyscrapers have many dozens of stories, have steel frames, make superb use of small footprint building areas, and offer hundreds of thousands of square meters of floor space. Roman villas suit a Mediterranean climate, and so on.

The development of an architectural style over time reflects the knowledge and experience gained by the builders and occupants as they try to meet a common set of requirements and accommodate the constraints of the local topography, weather, available building materials, tools, and labor. Ranch-style homes, such as those prevalent in Southern California, can be inexpensively built if lumber for framing is readily available, function very well in earthquake-prone areas, and are excellent for individuals who cannot climb stairs. Swiss chalets work well in areas with heavy snowfall, the steep roof assisting in minimizing the structural load caused by the snow. Therefore an approach that works well for providing homes in Southern California is not necessarily going to be appropriate for providing homes in Switzerland, or vice-versa. But within Southern California a wide variety of site-suitable homes can be successfully built

#### Vitruvius on styles

in a cost-effective manner by those architects skilled in the local idioms and materials.

"[Private buildings] are properly designed, when due regard is had to the country and climate in which they are erected. For the method of building which is suited to Egypt would be very improper in Spain, and that in use in Pontus would be absurd at Rome; so in other parts of the world a style suitable to one climate, would be very unsuitable to another; for one part of the world is under the sun's course, another is distant from it, and another, between the two, is temperate." Vitruvius, VI, 1, 1

One way architectural styles can be summed up is as a set of constraints – constraints put upon development in order to elicit particular desirable qualities. For example, the Swiss Chalet style has a constraint that the roofs have steep slopes; the quality elicited is that chalets tend to do well in areas of heavy snowfall. The suburban ranch style has a constraint that commodity components be used; the result being that the houses are cheaper to build and easier to fix than custom homes. The Gothic style constrains one to building with stone, stained glass, and high fluted vaults. The qualities elicited are that the buildings are inspirational, instructional, and long-lived.

Characterized in more constructive terms, styles offer the architect a wide range of solutions, techniques, and palettes of compatible materials, colors, and sizes. Rather than spending a large amount of time searching through an unbounded space of alternatives, by working within a style an architect can spend that same amount of time refining, customizing, and perfecting a particular design.

The concept of architectural styles carries over very powerfully into the domain of software. As we will illustrate in the remainder of this chapter and then throughout the book, styles are essential tools for architects to master, for they are a major point of intellectual leverage in the task of creating complex software systems.

#### 1.1.1 Limitations of the Analogy

Before pressing on to the detailed consideration of architectures, styles, and their use in software systems development, a few cautionary words are in order with regard to the use of the analogy to building architectures.

First, we know a lot about buildings. That is, since birth we have all experienced and learned about buildings. As a result we have a well-developed intuition as to what kinds of buildings can and cannot be built, and what is appropriate for a given need and situation. Our intuitions for

software are not nearly so well-developed and hence we must be more methodical and more analytical in our approach.

Second, the essential nature of the software medium is fundamentally different from the materials and media of building architecture. You can discern much of a building's architecture just by looking at it. With software the problem is much more difficult. Software is intrinsically intangible; at core it is an abstract entity and we only work with various representations of it. This implies that software is more difficult to measure and analyze, making it more difficult to evaluate the various qualities of designs and measure progress towards completion.

Third, software is more malleable than physical building materials, offering the possibility of types of change unthinkable in a physical domain. The building analogy is thus a poor source of ideas for dealing with change, since buildings accommodate change with difficulty<sup>1</sup>.

There are additional problems with the analogy:

- There is no software construction industry in the same sense that there is for buildings. Off-shore development is related, but the skill sets, training paths, and corporate organizations are not as mature or differentiated in the software domain as they are in the building domain.
- The discipline of architecture does not have anything akin to the issue of deployment as found in software: software is built one place, but deployed for use in many places, often with specialization and localization. "Manufactured buildings", a.k.a trailers, are somewhat similar, but still there is no corresponding notion to dynamic distributed, mobile architectures, as there is with software.
- Software is a machine; buildings are not (notwithstanding Le Corbusier's declaration that "A house is a machine for living in"). The dynamic character of software – the observation that led to Dijkstra's famous "goto statement considered harmful" paper, provides a profoundly difficult challenge to designers, for which there is no counterpart in building design.

Despite these limitations, the analogy between the architecture of buildings and software is strong and instructive. The focus on architecture is critical in the design of buildings; such a focus is similarly powerful for software. Subsequent sections of this chapter will demonstrate this: in

<sup>1</sup> This topic will be explored in more detail in Chapter 14. See "How Buildings Learn; What happens after they're built." Stewart Brand, Penguin Books, 1994.

the large, in the small, and in the crucible of industry. Before considering these examples, however, we summarize our main themes in the next section.

### 1.1.2 So What's the Big Idea?

The big idea is that software architecture must be at the very heart of software systems design and development. It must be in the foreground, more than process, more than analysis, and certainly more than programming. Only by giving adequate attention and prominence to the architecture of a software system, over its entire lifespan, can that system's development and long-term evolution be effective or efficient in any meaningful sense. Indeed, we will see that for any application of significant size or complexity, its architecture must be considered in advance, just as the successful creation of a large building requires consideration of its architecture in advance of construction.

Furthermore, the insights presented above about architecture, architects, and, especially, architectural styles offer substantial intellectual leverage in the creation of software systems, but demand careful study, good tools, and disciplined use to yield their substantial potential benefits.

Giving preeminence to architecture offers the potential for realizing:

- intellectual control
- conceptual integrity
- an adequate and effective basis for reuse – of knowledge, experience, designs, and code
- effective project communication
- management of a set of related variant systems

Note the phrase above about directing "attention and prominence to the architecture of a software system, *over its entire lifespan*." A limited-term focus on software architecture will not yield significant benefits. Just as the concept of architecture, or the involvement of an architect, in a building project is no guarantee that a successful building will be created, so it is for software. Shortcomings in the construction process – whether of buildings or of software – can cause the built system to deviate from its intended architecture, possibly with disastrous consequences. Such shortcomings can be avoided, however, and we will discuss techniques specifically intended to ensure that the implemented system is, and remains, faithful to its intended architecture.

Finally, it should be noted that by saying adequate attention must be given to a software system's architecture we are not advocating the creation of something wholly new: all software systems have an architecture. Just as every building has an architecture and at least one architect, so does software. Simply stating that a building, or a program, has an architecture

or an architect does not imply much. There are good architectures, bad architectures, elegant ones, and curious ones. So it is with software. An application's structure may be elegant and effective, or clumsy and dysfunctional. Our objective in the coming pages is to give the reader the skills necessary to ensure that applications have good, elegant, and effective architectures.

The following text proceeds by considering some outstanding examples of the discipline of software architecture, well applied.

## 1.2 The Power and Necessity of Big Ideas: the Architecture of the Web

A primary example of the power of architecture can be seen in an application all readers of this book are familiar with: the World-Wide Web. Think for a moment: what *is* the Web? How is it built? How do you explain the Web to a child? If you have a business and desire to have a Web-based e-commerce presence, how do you go about designing the software for your site, including determining how your site will interact with your customer's machines? It is architecture that offers the vocabulary and the means for answering these questions. It is the particular architectural style of the Web that constrains (and thereby helps) you in producing an e-commerce system that "plays well" with others.

Let's answer some of the questions above. What is the Web? In one view, focusing on the user's perception, the Web is a dynamic set of relationships between collections of information. In another view, focusing on coarse grain aspects of the Web's structure, the Web is a dynamic collection of independently owned and operated machines, located around the world, which interact across computer networks. In another view, taking the perspective of an application developer, it is a collection of independently written programs which interact with each other according to rules specified in the HTTP, URI, MIME, and HTML standards.

Considering these perspectives in turn, the view of the Web as a collection of interrelated pieces of information is illustrated in Figure 1-1.

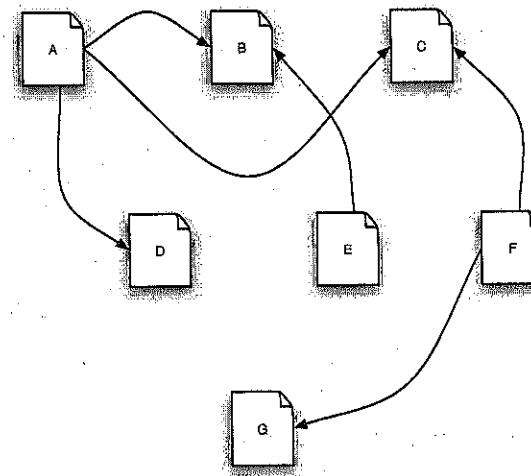


Figure 1-1, A document hypertext

In this diagram documents labeled A-G are shown as independent entities, but with explicit relationships between them. For instance, if document A is a biography of the author C.S. Lewis, then the arrow to document D might represent a view of The Kilns, the house in Oxford where Lewis lived for many years, as imaged by a webcam. The arrow to document C from document A might represent a reference to a description of Oxfordshire, the county in which The Kilns is found. The other documents shown might represent the text of some of the many books which Lewis authored, such as *The Lion, The Witch, and the Wardrobe*. We, as users of the Web, can understand this "mini-Web" as set of inter-related documents and a Web browser, such as Safari or Internet Explorer, as a vehicle for viewing these documents and navigating between them. In short this "mini-Web" is known as a *hypertext* and the viewing and shifting of focus from one document to the next as browsing, or "surfing", this hypertext.

The view illustrated in Figure 1-1 is one in which the data of the Web and the relationships between the data are shown. In contrast, Figure 1-2 shows the Web as a collection of computers interconnected through the Internet.

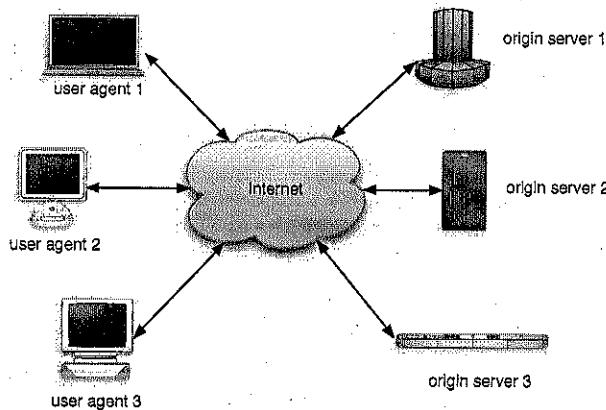


Figure 1-2. A "machine view" of a small part of the World Wide Web

The machines are shown here as being of two kinds: "user agents" and "origin servers". User agents are, for instance, desktop and laptop machines on which a Web browser is running. Origin servers are machines which serve as the permanent repositories of information, such as the aforementioned documents pertaining to C.S. Lewis. In this view the Web is understood as a physical set of machines whereby a user at a user agent computer can access information from the origin servers. The view is quite sketchy, however, and does not present any real insight into how the information in one document is related to information in another. Nonetheless the abstraction it presents is accurate insofar as it goes, and can be useful in explaining some Web concepts.

A third view of the Web is shown in Figure 1-3.

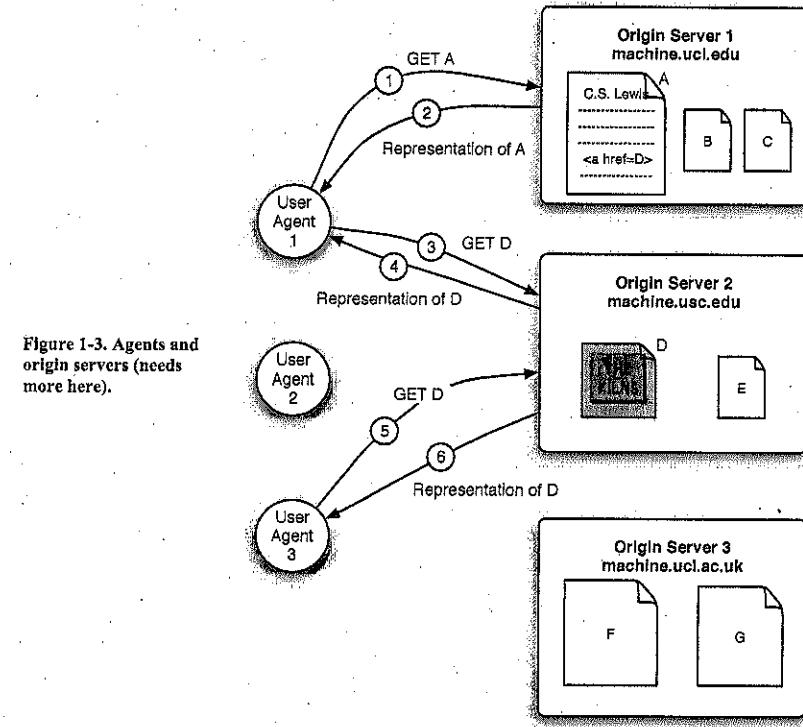


Figure 1-3. Agents and origin servers (needs more here).

In this view the user agents and origin servers of Figure 1-2 are once again shown, but now the location of documents A-G are shown. The figure also shows a set of specific interactions between two of the user agents and the origin servers, corresponding to a particular pattern of accessing the C.S. Lewis hypertext. In this example User Agent 1 requests, by means of the HTTP method "GET", a copy of document A, a biography of Lewis. This interaction is shown in the diagram by the arrow marked 1. A representation, or "copy", of the biography is returned, shown as 2. Since the biography has within it a hypertext reference ("href") to document D, a JPEG of The Kilns, User Agent 1 issues another GET, this time to machine.usc.edu, to obtain the picture. This request is marked 3 in the diagram. A copy of the image is returned, as shown in the arrow marked 4. Further interactions between user agents and servers are shown in the diagram as interactions 5 and 6.

These three diagrams illustrate the Web and provide an indication of how it works, but clearly there is much, much more to it. These diagrams use a very simple, limited set of information to represent the billions of pages of information available on the Web, and a set of less than a dozen machines to represent the millions of machines interacting at any given instant over the Internet. So, can we really say that these diagrams explain how the Web works? Clearly not. A much more general understanding of the Web can be given as a set of definitions and constraints on how these billions of documents interrelate and millions of machines interact<sup>2</sup>, as follows:

- The Web is a collection of *resources*, each of which has a unique name known as a uniform resource locator, or “URL”.
- Each resource denotes, informally, some information. Any information that can be named can be a resource. This can be, for example, a document, an image, a time-varying service (e.g., “today’s weather in Los Angeles”), a collection of other resources, and so on.
- URL’s can be used to determine the identity of a machine on the Internet, known as an *origin server*, where the value of the resource may be ascertained.
- Communication is initiated by clients, known as *user agents* who make requests of servers. Web browsers are common instances of user agents.
- Resources can be manipulated through their *representations*. For instance, a resource may be updated by a user agent sending a new representation of that resource to the origin server that holds that information. Similarly a resource may be viewed by a user agent obtaining a representation from an origin server and displaying that representation on a monitor. HTML is a very common representation language used on the Web.
- All communication between user agents and origin servers must be performed in accordance with a simple, common protocol (HTTP). Communicating according to HTTP requires that the parties implement a few primitive operations, such as GET and POST.
- All communication between user agents and origin servers must be context-free. That is, an origin server must be able to respond correctly to a user agent’s request based solely on information contained in the request, and not require maintenance of a history of interactions between that user agent and the origin server. (This is sometimes known as “stateless interactions”.)

<sup>2</sup> This characterization, still omits many details, of course! A much more comprehensive description appears in Chapter 11.

In the example above, documents A-G are resources; machines “machine.uci.edu” and “machine.usc.edu” running the Apache web server are example origin servers. User agents could be personal laptops running a web browser such as Internet Explorer. Representations include a copy of the HTML of Lewis’s biography, and a .jpg of the current view of The Kilns as imaged by a webcam.

While the list above shows many of the principal design decisions governing the Web, it is not a complete list. To fully characterize the Web we would have to decide on a particular moment in time, determine the various machines on the Internet which were interacting according to the Web protocols, and determine the key characteristics of the multitude of software applications configured to act as user agents, origin servers, and so on. By describing, instead, the rules by which the various parts of the Web work and interact – its architectural *style* – we provide the basis for understanding the Web independent of its configuration or actions at any particular instant. The description given above enables us to reason about how the Web works and guides in determining what must be done to incorporate new information or new machines into the Web.

A number of critical observations are apparent.

- The architecture of the Web is wholly separate from the code that implements its various elements. Indeed, to understand the Web the architecture is the *only* effective reference point. The architecture is the set of principal design decisions which determine the key elements of the Web and their interrelationships. These decisions are at an abstraction level above that of the source code, and are thus conducive to understanding the whole system at the application level.
- There is no single piece of code that “implements the architecture”. The Web is “implemented” by Web servers of various design, browsers of various design, proxies, routers, and network infrastructure. Just looking any single piece of code, or even all the code on any single machine, will not explain the Web’s structure; rather the architecture is the only adequate guide to understanding the whole.
- There are multiple equivalent (with respect to the architecture) pieces of code that exist and implement the various components of the architecture. The architectural style of the Web constrains the code in some respects, saying how a given piece must work with respect to the other elements of the architecture, but substantial freedom for coding the internals of an element is present. Thus we see many different browsers from different vendors, offering a variety of individual advantages, but insofar as the browsers relate to the rest of the Web, they are equivalent.

- The stylistic constraints that constitute the definition of the Web's style are not necessarily apparent in the code, but the effects of the constraints as implemented in all the components are evident in the Web.

These observations are profound, and begin to indicate the role of architecture in the Web. But the most important questions of all remain:

- Why were these particular decisions made?
- Why were these decisions important and not others?
- Why did similar systems that made slightly different decisions fail, when the Web is such a wild success?

These questions can only be answered when looking at the Web from an architectural perspective, and indeed they cut straight to the heart of architecture. In Chapter 11 we will see how the Web's designers targeted a particular set of qualities - the ones that make the Web so successful - and then made these decisions specifically to imbue the Web with those qualities. That chapter will discuss the Web and its underlying style, REST, in more detail, and show how the style is based upon and derivative from a large set of simpler styles.

The take-away message here is that one of the world's most successful software applications is only understood adequately from an architectural vantage point. The development of the Web, the maturation of the HTTP/1.1 protocol, and the implementation of its core elements were all driven by architectural understandings and principles. Without the rock of this abstraction it is unlikely the Web would have survived past its first two or three years of existence.

### 1.3 The Power of Architecture in the Small: Architecture on the Desktop

One need not look at large complex applications, such as the Web, to find interesting architectures, or to find applications where a focus on architectures has a big payoff.

Architectures underlie the simplest applications, and architectural concepts provide the conceptual power behind, for example, the nearly ubiquitous command-line "shell" programs. Found on virtually every platform, including Mac OS X, Linux, Windows, as well as the Unix platforms where the concepts originated, such scripts enable the user to quickly and easily compose new applications from pre-existing components (programs), called "filters", following some simple rules. For example, the following application creates a sorted list of all the files in the directory named "invoices" whose names include the phrase "August":

```
ls invoices | grep -e August | sort
```

At first blush this may not seem to be an "application", since we can visually discern how the functionality is provided from piece-parts, but that is indeed what it is. To understand how this application works and how it is built, one must understand in general what "filters" and "pipes" are, understand what the specific filters used in building this application do, and lastly reason about how these particular filters are configured, using the pipes, to form this application.

First, a "filter" is a program that takes a stream of text characters as its input and produces a stream of characters as its output. A filter's processing may be controlled by a set of parameters. A "pipe" is a way of connecting two filters, in which the character stream output from the first filter is routed to the character stream input of the second filter.

In the application above, three filter programs are used: `ls`, `grep`, and `sort`.

`sort` examines its input stream, noting how the stream is divided into lines of text by an end-of-line character, and produces on its output stream those same lines of text, but in sorted order. While `sort` may be given optional parameters to control, for instance, whether the lines are sorted in ascending or descending order, in the application above no parameters are provided, so the default values are used (*viz.*, to sort in ascending order).

`grep` examines its input character stream for lines (i.e. portions of the input character stream demarcated by end-of-line characters) which contain a sub-string matching a string value provided as a parameter. In the application above the `-e` parameter is used to provide the string value ("August") for which `grep` is to search. `grep` produces as its output stream only those lines that contain the designated search string.

`ls` does not process an incoming stream of characters; instead it communicates with the operating system to obtain the names of files in a named directory (or "folder"). `ls` then produces, as its output stream, a sequence of characters which are the textual names of the files in the directory designated by the command line parameters to `ls`, with each file name followed by an end-of-line character.

With this understanding of filters (programs that read and produce character streams), pipes (ways of hooking up filters by routing the character streams) and the functioning of each of the three filters used (listing file names, looking for the presence of a particular substring, and sorting), it is easy to understand how the application above works. `ls` produces a textual list of files found in the `/home/invoices` directory. A pipe (shown on the command line as a vertical bar) routes this output to

the input of `grep`. `grep` then examines those names to identify any containing the sub-string "August", and produces only those names as its output stream. A second pipe routes that output stream on to `sort`, which then sorts the file names in ascending order, producing that ordered listing as its (and the application's) output.

The critical observation here is that this application's structure can be understood on the basis of a very few rules. Given understanding of that structure and knowledge of the functioning of the individual filters, the function of the complete application can be understood. Knowledge of those same rules and of the functioning of a few dozen, pre-existing, basic filter programs allows one to understand hundreds of other useful applications. Similarly, a developer may readily create new applications based upon those same rules and knowledge of the filters.

These commonly used Unix filter programs can be used individually or combined into pipe-and-filter architectures to create many useful applications. Consult your system's manual pages for detailed instructions on how to use them (try "man man" in a terminal window).

`ls`: lists the names of files within a directory.  
`grep`: produces lines on output that match a specified pattern, where that pattern is described as a regular expression.  
`sort`: sorts all input lines according to a set of parameters (e.g. for ascending or descending order).  
`cat`: concatenates files specified by parameters to the output stream.  
`sed`: reads the input stream, modifies (edits) it according to specified parameters, and writes the result to the output.  
`awk`: matches patterns in the input stream and performs specified operations upon a match.  
`head`: lists the first n lines of the input file on the output.  
`tail`: lists the last n lines of the input file.  
`uniq`: copies unique input lines to the output.  
`less`: incrementally lists input file on the output, with controls determining how much information to list at a given time.  
`lpr`: input files are sent to the printer.  
`cut`: selects portions of each input line and writes them to the output.  
`man`: formats and displays the on-line manual pages for a specified command to the output.  
`tee`: copies the input to the output, plus makes a copy in zero or more specified files.

A complex example  
`grep HTTP_USER_AGENT httpd_state_log | cut -f 2-`

#### Common Unix filter programs

```
grep -v 'via Gateway' | grep -v 'via proxy gateway' | sort | uniq -c | sort -nr | head -5
```

This produces the top 5 browsers ("user agents") from a WWW state log called "httpd\_state\_log" excerpting all proxy user agent strings.

The particular set of rules at work here define an architectural style known, not surprisingly, as pipe-and-filter. Part of the beauty of pipe and filter is that, because of its simplicity, end users can develop applications without ever being trained as "programmers". It is akin to working with Lego blocks, or Tinker Toys: once you understand how to fit the parts together, and the different kinds of functions that the various piece-parts are capable of performing, the creative task of assembling the pieces into a new design can proceed quickly and effectively. Training in the details of programming is not required; the power of a simple architectural concept can be comprehended and applied by a broad audience.

Though the style is very simple, note that use of it is not confined to the use of the standard filter programs found in Unix, Linux, and the other operating systems that support pipe and filter; a developer may create a program that operates by reading and writing a character stream and then use that filter/program in conjunction with others in a pipe and filter-based application. Similarly the style is not confined to applications written in the command-line notation, though that notation is certainly common.

In addition to pipe and filter, a wide variety of other simple architectural styles exist. Most of these will be familiar to experienced developers: layered system, main program and subroutines, object-oriented, implicit invocation, and blackboard. A detailed discussion appears in Chapter 4. Developers can choose among these styles, and a vast array of others, based upon the nature of the problem to be solved and the qualities desired in the solution. For instance, pipe and filter applications are readily understandable, run on almost any operating system, and run efficiently when the problem (and its structuring in pipe and filter) admits concurrency. On the other hand pipe and filter requires all communication between filters to be serialized into character streams; thus if a graph data structure has to be "passed" from one filter to another it must first be serialized into a textual stream, transferred across the pipe, and then rebuilt into the graph data structure by the next filter. The pipes ensure syntactic compatibility between the filters, but do nothing to ensure semantic compatibility.

## 1.4 The Power of Architecture in Business: Productivity and Product Lines

The discussion of the WWW in section 1.2 illustrated how architecture is a critical enabler for the development of large-scale, complex systems. The discussion of the pipe and filter style in section 1.3 showed how architectural concepts can make effective the development of even one-line applications, providing the leverage needed for exploiting the power of a library of reusable components (in particular, Unix “filters”). Architectures are also critical enablers for developing *product families*, a key element of many business strategies.

Product families are sets of independent programs which have a significant measure of commonality in their constituent components and structure. An example will serve to indicate the key concepts. As any purchaser of consumer electronics, such as televisions, is aware, a myriad of choices are available. Even from a single manufacturer, the consumer is faced with a range of sizes and features that allows one to purchase a device meeting a very particular set of requirements. A purchaser might be interested in obtaining, e.g., a 35-inch HDTV with a built-in DVD player for the North American market. Such a device might contain upwards of a million lines of embedded software. This particular television/DVD player will be very similar to a 35-inch HDTV without the DVD player, and also to a 35-inch HDTV with a built-in DVD player for the European market, where the TV must be able to handle PAL or SECAM encoded broadcasts, rather than North America’s NTSC format. These closely related televisions will similarly each have a million or more lines of code embedded within them.

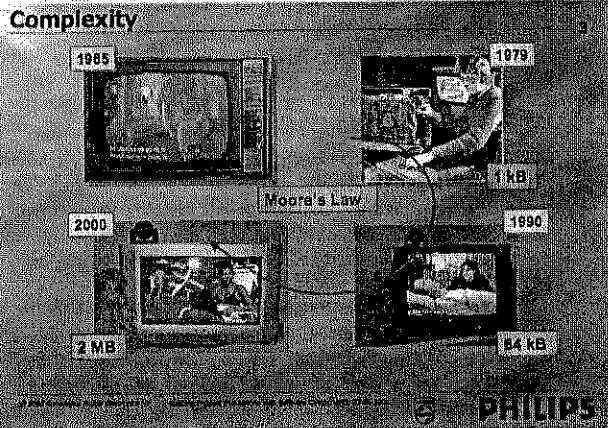
The economic challenge from the manufacturer’s point of view is to produce the wide range of products that a world-wide market of sophisticated consumers demands while simultaneously exploiting the commonalities between members of a product family. Reusing structure, behaviors, and component implementations is increasingly important to successful business practice because

- it simplifies the software development task: existing design- and implementation-level solutions can be either directly applied or easily adapted to multiple products within a family;
- it reduces the development time and cost: part of the functionality needed for a new product will already exist within previous products within the same family; and
- it improves the overall system reliability: any functionality that is reused from a previous product will have been used and tested more extensively than if developed anew.

Software architecture provides the critical abstractions that enable variation and commonality within a product family to be simultaneously managed. We will provide an extensive treatment of this subject in Chapter 15. Here we discuss a representative example that demonstrates the power of product families and the benefits accrued via an explicit, and extensive, software architectural focus.

The business case for exploiting software architecture for this task has been recognized by one of the world’s leading consumer electronics manufacturers, Philips. Since the late 1990’s Philips has progressively developed and applied their Koala technology for specifying and implementing the architectures of their mid- and high-end television sets, and has hundreds of software engineers exploiting the concepts.

The motivation for Koala came directly from the nature of advances in the consumer electronics domain. An example of this is depicted in the case of Philips television sets in Figure 1-4. While early TVs supported a very small number of simple functions, over time they became more powerful, with increasingly sophisticated hardware and, eventually, software capabilities. The resulting growth in complexity carried with it the risks of ever-increasing costs and times-to-market. Of course, this is precisely the opposite of what modern consumers have come to expect: fierce competition has forced Philips, as well as its rivals, to produce a steady stream of new products and variations on existing products, while containing their costs.

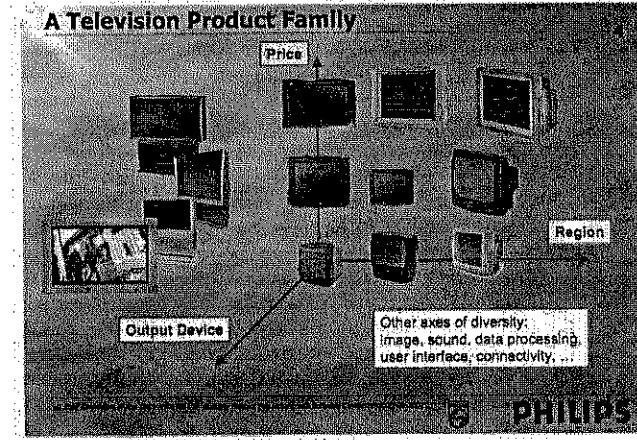


**Figure 1-4.** More sophisticated products carry with them greatly increasing complexity, which in turn implies greatly increasing cost and worse time-to-market unless the problem is addressed.

@@@Diagram supplied by Rob van Ommering, but no explicit permission has been requested or granted for use in this manuscript to date@@@

**Figure 1-5.** Philips TVs as a product family, varying along the three dimensions, but with significant commonality among members.

@@@Diagram supplied by Rob van Ommering, but no explicit permission has been requested or granted for use in this manuscript to date@@@

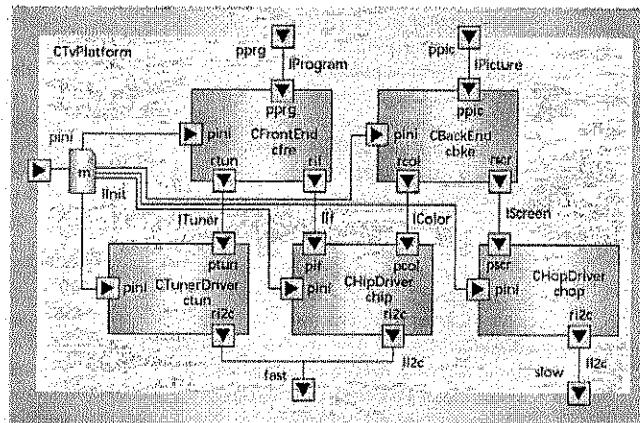


Philips addressed the problem by formulating a product family in which its many different types of TV sets varied along the three dimensions depicted in Figure 1-5 – price, output device, and geographical region – while they shared their basic purpose and much of their functionality. The same approach was applied to other Philips products: VCRs, DVD players, audio equipment, and so on.

In order to support its product families adequately, Philips had to be able to address two key issues: *commonality* and *variability* across products. The key observation that the Philips engineers made, and one that is of particular relevance to this book, was that the product family notion extended to the growing amounts of *software* embedded in the different devices. To exploit the commonality and manage the variability across the different embedded software product families, Philips developed an architectural methodology, called Koala. A more extensive treatment of Koala is provided in Chapter 15. Here we only highlight its key features.

Koala models and implements a software system as a collection of interacting components. Each component exports a set of services via a set of *provides* interfaces. Additionally, each component explicitly defines its dependencies on its environment (either the hardware or other software components) via a set of *requires* interfaces. For illustration, a software architecture for a Philips TV platform modeled in Koala's graphical notation is shown in Figure 1-6.

**Figure 1-6.** An example software architecture for a TV set. The architecture consists of five interacting components with various incoming and outgoing interfaces (denoted by the direction of the corresponding arrow). @@Diagram supplied by Rob van Ommering, but no explicit permission has been requested or granted for use in this manuscript to date@@



This approach allows an engineer to construct and analyze an architecture with relative ease: each component is essentially akin to a Lego block with well defined “pins” for composing with other components; in order for such compositions to be legal, the *provides* and *requires* interfaces of the respective components must match according to a set of rigorously defined rules. Moreover, a given architecture constructed in Koala is treated as a *compound component*, which can then be used as a single unit. For example, the architecture shown in Figure 1-6 is a compound component with two *provides* and two *requires* interfaces. This allows components of arbitrary complexity to become reusable assets across Koala architectures (that is, across Philips products).

Our previous examples of the use of software architecture, the Web and pipe-and-filter applications, hints that a focus on architecture is a focus on reuse: reuse of ideas, knowledge, patterns, and well-worn experience. In turn, product family architectures facilitate a higher-order level of reuse: reusing structure, behaviors, implementations, and so on, across many related products.

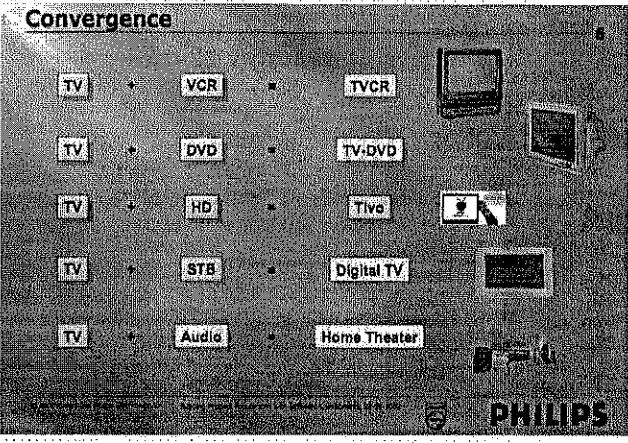
In addition to its ability to exploit commonalities within a product family via reusable assets, Koala also provides explicit support for managing variability across products. Three separate mechanisms are used to this end:

1. *Diversity interfaces* are a mechanism for parameterizing a component. Diversity interfaces allow a component to “import” configuration-specific properties from Koala’s specialized interface implementation elements, which are external to the

component and are contained within the architecture encompassing the component.

2. *Switches* are connecting elements that allow a single component to interact with one of a set of components, depending on the value of a given runtime parameter.
3. *Optional interfaces* allow a component of a given type either to provide or to require additional functionality that may be specialized for certain, but not all, products within a family.

The combination of Koala’s support for sharing reusable assets of arbitrary complexity and managing diversity across products in a family has made it possible for Philips to explore combining components from different families in novel and interesting ways. Some of those are depicted in Figure 1-7. The resulting *product populations* are a further extension of the technical challenges inherent in product families. For example, the presence of variation induces requirements for extensive configuration management of the individual components and of entire architectures.



**Figure 1-7.** An ever expanding range of possibilities opens by combining existing consumer electronics products. This provides an even broader and longer-term motivation for product families.

@@Diagram supplied by Rob van Ommering, but no explicit permission has been requested or granted for use in this manuscript to date@@

Koala has directly helped Philips to conquer these challenges and turn them into a competitive advantage. We should note that while architecture has played a central role in this process, product families and populations also require broader changes to processes and business organization practices. The standard approach to software development as found in

most businesses does not effectively support product families. One common reason is that a development team often has little incentive to expend its already scarce resources and produce more widely (re)usable assets that will benefit other teams and projects in the future. Therefore, introduction of a robust strategy to support product families also demands changes in how development organizations are structured and operate internally, and how they interact with other parts of a company's business, including marketing, hardware engineering, and finance.

Apart from the obvious cost savings that accrue due to the reuse of components and the ability to quickly craft yet another new television configuration, the Philips example reveals another critical benefit of the software architecture abstraction: Koala is the concrete manifestation of the company's corporate experience, knowledge, and competitive advantage. Without a specific way of representing such knowledge, companies are left relying on the memories of their employees and the verbal conveyance of past experience to retain and pass along "our company's way" of solving problems and creating new products. With increasing trends of employee mobility from company to company, reliance on a social structure to maintain such understanding is an increasingly shaky policy. Software architecture offers not only a solution to a socially-induced problem, but, with its substantial technical support, the ability to achieve much higher levels of productivity than have heretofore been seen. This is a critical observation and further explication of it will be provided throughout the remainder of this book.

## 1.5 End Matter

The character of architecture

"Architecture depends on fitness (ordinatio) and arrangement (dispositio), ... it also depends on proportion, uniformity, consistency, and economy."  
"Vitruvius I, 2, 1."

This chapter began with an extended discussion of the analogy between the way buildings are designed and constructed and how software is designed and built. The fundamental role of architecture has been emphasized throughout the chapter, showing its essential role in the World Wide Web, and then, at the other end of the size spectrum, in quickly-composed desktop applications. The chapter has concluded with a discussion of product families. This concluding focus is particularly appropriate as it echoes closely a lesson from the world of buildings, namely the critical role of architecture and architects in carrying forward lessons, experiences, and reusable elements to new projects.

In 1979 the architect Christopher Alexander published a book entitled, *The Timeless Way of Building*. In it, he shows how patterns of solutions to common architectural needs have developed over the years, and how combinations of patterns can be made to yield structures that address complex needs and constraints. Software architecture not only supplies the intellectual means for applying such reuse of knowledge in the software domain, enabling engineers to efficiently address needs for new systems, but also provides the framework for reusing substantial functional components in the production of new members of a product family.

The vision of architecture-centric software engineering is very compelling. It prefigures a world where complex software systems are engineered, rather than crafted, drawing from extensive experience in past projects to form the basis for new ones. System designs are modeled in a variety of notations, each optimized for depicting particular aspects of the architecture. Powerful tools automate the process of maintaining consistency between these models. Each project stakeholder has a panoply of visualizations available for looking at the architecture in ways that are most natural or convenient. Capable analysis tools provide deep insights into the nature of the designed system long before implementation activities begin—stakeholders are able to assess the qualities of a software system from its design before costly mistakes are introduced. The design serves as the basis for system deployment and evolution as well, informing future engineers as to exactly how to evolve the system in ways that are consistent with its original design principles and goals. The architecture (and the qualities induced by it) accompanies the system through its lifetime to its eventual retirement. This vision is not fully a reality today. However, as this book will show, today's foundations, theory, and practice of software architecture can achieve vastly superior results to those of traditional development practices, while also providing a rich basis for achieving the stated vision.

The coming chapters will supply the missing details in our discussion. To apply the techniques of software architecture one must have adequate conceptual foundations, notations, analysis techniques, tools, and processes, all of which will be discussed. We will begin this examination in the next chapter by considering how a software architecture-centric approach to development radically reshapes the other tasks and processes of software engineering.

## 1.6 Review Questions

1. What are the principal insights from the discipline of building architecture that are applicable to the construction of software systems?

2. Recognizing the limitations of an analogy – where it does not apply – can be as instructive as considering the situations where it does apply. What's wrong with the architecture analogy? In what ways is constructing software fundamentally different from building a physical structure? Do a Google search on "software construction analogy is broken". Do you agree or disagree with the opinions posted online?
3. Philips' use of software architecture for supporting product lines is targeted at consumer electronics, such as televisions. What other industries or markets could benefit from the commonalities and efficiencies of a software product-line approach?

## 1.7 Exercises

1. Architects use hand-drawn sketches, prose, and blueprints to describe buildings. What do these correspond to in software development?
2. When a software developer begins a new development task by directly starting to program, what kind of development activity would that correspond to in building?
3. Look up several definitions of "software design". Do any of these definitions correspond to what architects (or industrial designers) term "design"?
4. What corresponds in software development to a building architect's concern for aesthetics?
5. Interview an architect and find what their key vocabulary items are. From your knowledge of software engineering, what analogs do those terms have in software?
6. Is  $X$  a better analogy for the construction of software? Why or why not? Let  $X = \{\text{law, medicine, automotive engineering, oil painting}\}$ .
7. Do a Web search of "software architecture". Are the top hits deserving of the billing? Are the terms used on those Web sites consistent with the terms as used in this textbook?
8. Write a pipe and filter application prints a sorted list of every unique word in a file. I.e. each unique word should appear only once on the output.

## 1.8 Further Reading

The works of Vitruvius have been translated into English many times and should be readily available in a good library. Free, on-line translations are also available; see for example Bill Thayer's website[230].

Many excellent books on architecture have been written, of course, but few provide substantive insights for software developers. A significant exception is Stewart Brand's *How Buildings Learn* [27]. Brand chronicles how a wide range of kinds of buildings have been changed over the many years since their initial construction. A discussion of some of the

principles from this book and how they relate to software architecture is found in Chapter 14 of this text. Another architecture text that has had substantial impact on software development is Alexander's *The Timeless Way of Building* [8]. This work has influenced thinking on patterns for object-oriented programming, and more generally, software architecture styles.

An interesting chronicle of the construction of a New York City skyscraper can be found in [248]. The processes the designers and builders follow, and the problems they encounter, are eerily similar to those in large-scale software development.

A detailed discussion of the architecture of the World Wide Web can be found in [76]. Key points from this work are discussed in detail in Chapter 11. The standards that govern the operation of the web are available from the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) web sites: [www.ietf.org](http://www.ietf.org) and [www.w3.org](http://www.w3.org), respectively. Tim Berners-Lee's description of the Web from 1994 can be found at [18].

Further information on Koala and how it has been used to support development of product families is available at [213] and [298].

## CHAPTER 2

## 2 Architectures in Context: The Reorientation of Software Engineering

The preceding chapter introduced the concept of software architecture and illustrated its power in establishing the contemporary World Wide Web. It also showed how software architecture provides a technical foundation for the exploitation of the notion of product families. This chapter shows how software architecture relates to the concepts of software engineering that traditionally are the most prominent.

What emerges from this consideration is a reorientation of those concepts, for the power of architecture demands a primacy of place. As a result the very character of key software engineering activities, such as requirements analysis and programming, are altered and the technical approaches taken during various software engineering activities are changed.

Since the focus of this chapter is showing the role of architecture in the whole of the software engineering enterprise, it is somewhat cursory – most of the major topics of software engineering are discussed, but each individual topic is only allotted a few pages. Subsequent chapters will take up the major points in turn, treating them in substantial detail. The reader will be able to understand the role of software architecture in the larger development context, and could apply the ideas in broad terms, but without the techniques and tools covered in subsequent chapters effective application of the ideas will be elusive.

## Outline of Chapter 2

- 2 Architectures in Context: The Reorientation of Software Engineering
- 2.1 Fundamental Understandings
- 2.2 Requirements
- 2.3 Design
  - 2.3.1 Design techniques
- 2.4 Implementation
  - 2.4.1 Implementation strategies
- 2.5 Analysis and Testing
- 2.6 Evolution and Maintenance

- |  |  |
|--|--|
|  | <ul style="list-style-type: none"> <li>2.7 Processes</li> <li>2.7.1 The Turbine Model</li> <li>2.8 End Matter</li> <li>2.9 Review Questions</li> <li>2.10 Exercises</li> <li>2.11 Further Reading</li> </ul> |
|--|--|

### 2.1 Fundamental Understandings

There are three fundamental understandings of architecture, the recognition of which helps situate architecture with respect to the rest of software engineering:

1. Every application has an architecture.
2. Every application has at least one architect.
3. Architecture is not a phase of development.

By architecture we mean the set of principal design decisions about a system; the blueprint or characterization of the essence of the application. Referring back to the analogy to buildings discussed at the beginning of the previous chapter, it is evident that every building has an architecture. That is not to say that every building has an honorable, or elegant, or effective architecture: sadly, many buildings evince architectures which ill-serve their occupants and shame their designers. But those buildings *have* architectures, just as much as the beautiful, elegant buildings which are a delight to see and to work within. So it is with software. An application's fundamental structure can be characterized, and the principal design decisions made during its development can be laid out. For example, as described in the previous chapter, the architecture of the World Wide Web is characterized by the set of decisions referred to as the REST architectural style. The Unix shell script we saw in the previous chapter has an architecture characterized by the pipe-and-filter style. All applications do have architectures.

The contribution of this observation is that it immediately raises questions: where did the architecture of an application come from? How can that architecture be characterized? What are its properties? Is it a "good architecture" or a "bad architecture"? Can its shortcomings be easily remedied?

The second understanding follows naturally from the first: every application has an architect, though perhaps not known by that title or

recognized for what is done<sup>3</sup>. The architect is the person or, in most cases, group who makes the principal decisions about the application, who establishes and (hopefully) maintains the foundational design. As with the first understanding, this observation also immediately raises some questions, including: Were the architects always aware when they had made a fundamental design decision? Can they articulate those foundational design decisions to others? Can they maintain the conceptual integrity of the design over time? Were alternatives considered at the various decision points?

The third understanding is the most profound, and which provides the focus for the majority of this chapter. Architecture refers to the conceptual essence of an application, the principal decisions regarding its design, the key abstractions that allows one to characterize the application. If it is agreed that every application has an architecture, then the question arises, where did it come from? How does it change?

In a simplistic, traditional, and *inaccurate* understanding, the architecture is a specific product of a particular phase in the development process that follows identification of requirements and which precedes detailed design. In elaborate software engineering waterfall processes, or in the spiral model, such phases are often explicitly labeled, using such terms as “preliminary design”, “high-level design”, “product design”, or “software product design”. Thinking of architecture as the product of such a phase – especially an early phase – confines architecture to consist of only a few design decisions, a subset of those that fully characterize the application, and, unfortunately in many cases, to the decisions most likely to be contravened by subsequent decisions. While the creation and maintenance of the architecture may begin or have special prominence in a particular phase, these activities pervade the development process.

To show how software architecture relates to the broader traditional picture of software engineering, we discuss architecture in the context of traditional phases and activities of software engineering. For convenience and familiarity, we organize the following discussion around the notional waterfall process. Our discussion is predicated on a recognition that a system’s architecture should result from a conscious, deliberate activity by an individual or group recognized as having responsibility for the architecture. Those unfortunate situations where the architecture is not

<sup>3</sup> Conversely, just because a company bestows a title such as “chief software architect” on someone does not necessarily mean that the individual possesses any particular credentials or ability to responsibly create good or effective software architectures, or indeed to know anything about software technology.

explicit and not the result of conscious choice or effort simply reflect poor engineering practice.

## 2.2 Requirements

Consideration of architecture rightly and properly begins at the outset of any software development activity. Notions of structure, design, and “solution” are quite appropriate during the requirements analysis activity. To understand why, it is appropriate to begin with a short exploration of the traditional software engineering approach. We contrast that view with the practice in actual software development, the practice in (building) architecture, and then consider the role of design and decision making in the initial phase of application conception.

In the waterfall model, indeed in most process models, the initial phase of activities is focused on developing the requirements for an application – the statement of what the application is supposed to do. The traditional academic view of requirements analysis and specification is that the activity, and the resulting requirements document, should remain unsullied by any consideration for a design that might be used to satisfy the identified requirements. Indeed, some researchers in the requirements community are rather strident on this point: “The central part of this paper sketches an approach to problem analysis and structuring that aims to avoid the magnetic attraction of solution-orientation”[139]; similar quotes can be found throughout the literature. (More recent work in requirements engineering has moved away from such a viewpoint, as will be discussed at the end of the chapter.)

The focus on isolating requirements and delaying any thought of solution goes back to antiquity. Pappus, the Greek mathematician from the fourth century wrote: “In analysis we start from what is required, we take it for granted, and we draw consequences from it, till we reach a point that we can use as [a] starting point in synthesis.” Synthesis is here the design, or solution, activity. More recently, the twentieth century American mathematician Polya wrote an influential treatise on “How to Solve it” [231]. The essence of his approach is:

- First, understand the problem.
- Second, find the connection between the data and the unknown. You should obtain eventually a plan of the solution.
- Third, carry out your plan.
- Fourth, examine the solution obtained.

In both these approaches, a full understanding of the requirements precedes any work towards solution. Most software engineering writers have taken this essential stance, as we have seen in the quote above, and

argued that any thought about how to solve a problem must follow a full exploration and understanding of the requirements.

One of the stories used to illustrate the wisdom of this approach concerns the development of washing machines. If in designing washing machines we simply automated the manual solution of ages past we would have machines that banged clothes on rocks down by the riverside. In contrast, focusing on the requirements (namely, cleaning clothes) independent of any “magnetic attraction of solution-orientation” allows novel, creative solutions to be obtained: rotating drums with agitators.

This ideal view of isolating requirements first, then designing afterwards, is in substantial contrast to the typical practice of software engineering. While it is not something that developers write academic papers about, the practice indicates that, apart from government contracted development and some specialized applications, substantive requirements documents are seldom produced in advance of development. Requirements analysis, which ostensibly produces requirements documents, is often done in a quick, superficial manner, if at all. Explanations for such deviation of actual practice from putative “best practices” include schedule and budget pressures, inferior processes, denigration of the responsible engineers’ qualifications and training, and so on.

We believe the real reasons are different, and that these differences begin to indicate the role of architecture and solution considerations at the very outset of a development process. The differences have to do with human limitations in abstract reasoning, economics, and perhaps most importantly, “evocation”.

Consider once again the analogy to buildings. When we decide we need a new house or apartment, or a modification to our current dwelling, we do not begin a process of reasoning about our needs independently of how they may be satisfied. We think, and talk, in terms of how many rooms, what style of windows, whether we want a gas or electric stove – not in terms of “means for providing shelter from inclement weather, means for providing privacy, means for supplying adequate illumination, means for preparing hot food” and so on. We have extensive experience with housing, and that experience allows us to reason quickly and articulately about our desires, and to do efficient approximate analyses of cost and schedule for meeting the needs. Our seeing other houses or buildings inspires our imagination and sparks creative thought as to what “might be”. Our needs start to encompass particular styles of houses that we find charming, or “cutting edge.” Thus our understanding of the architecture of our current dwelling and the architecture of the other people’s dwellings enables us to envision our “needs” in a way that is likely to lead to their satisfaction (or revision downwards to reality!).

So it is with software. Specifying requirements independently of any concern for how those requirements might be met leads to difficulty in even articulating the requirements. Aside from limited domains, such as numerical analysis, it is exceptionally difficult to reason in purely abstract terms. Without reference to existing architectures it becomes difficult to assess practicality, schedules, or cost. Seeing what can be done in other systems, on the other hand, what kind of user interfaces are available, what new hardware is capable of, what kind of services can be provided, evokes “requirements” that reflect our imagination and yet which are grounded in reasonable understandings of possibility. Current practice reflects this approach, showing the practicality of reasoning about structure and solution hand-in-hand with requirements.

This observed experience with software practice is consistent with what is found in other engineering disciplines. Henry Petroski, the popular chronicler of the modern history of engineering, has observed that failure is the driver of engineering and the basis for innovation. That is, innovation and new products come from observation of existing “solutions” and their limitations. Reference to those prior designs is intrinsically part of work towards new solutions and products.

#### The Development of Zippers

The nearly ubiquitous zipper followed a typical engineering development path. Rather than starting from a “design free” functional specification – something like “means for joining edges of jacket” – the zipper appeared in the early 1900’s as an incremental successor to a long line of patented inventions. The earliest of these go back to the problem of buttoning high-top boots. From the C-curly hook-and-eye fastener to the Plako to the “hidden hook” and then to the still-common nested, cup-shaped fasteners we refer to as zippers, the history is one of repeated invention, failure, and new innovation. In addition to the technical challenges of getting a fastener to function reliably and be aesthetically acceptable, the developers of the zipper also faced the equally daunting challenge of developing a demand for the product.

Petroski tells the story in detail in “The Evolution of Useful Things”. He concludes his chapter on the zipper with the following insight, “...like the form of many a now familiar artifact, that of what has come to be known as the zipper certainly did not follow directly from function. The form clearly followed from the correction of failure after failure.”

Similarly, if we consider the behavior of corporations, or especially of venture capitalists, we see a focus from the outset on structures and designs, rather than requirements. That is, one does not successfully approach a venture capitalist and simply enumerate a great list of

requirements for some product. Requirements do not create value; products do. Successful new ventures are begun on the basis of a potential solution – possibly even without a conception of what “requirement” it might be meeting. Marketing organizations within companies have as their charter the responsibility to match existing products to needs, to create “needs”, or, especially to identify how existing products need to be modified in order to address emerging customer needs. In all this, solution and structure are equal partners with requirements in a conversation about needs.

The core observations from this reflection are:

- Existing designs and architectures provide the vocabulary for talking about what might be;
- Our understanding of what works now, and how it works, affects our wants and perceived needs, typically in very solution-focused terms;
- The insights from our experiences with existing systems helps us imagine what might work and enables us to assess, at an early stage, how long we must be willing to wait for it, and how much we will need to pay for it.

The simple conclusion then, is that analysis of requirements and consideration of design – concerning oneself with the decisions of architecture – are naturally and properly pursued cooperatively and contemporaneously.

The starting point for a new development activity thus includes knowledge of what exists now, how the extant systems fail or fail to provide all that is desired, and knowledge of what about those systems can or cannot be changed. In many ways, therefore, the current architectures drive the requirements. Indeed, requirements can be thought of as the articulation of improvements needed to existing architectures – desired changes to the principal design decisions of the current applications. Architectures provide a frame of reference, a vocabulary, a basis for describing properties, and a basis for effective analysis. New architectures can be created based upon experience with and improvement to pre-existing architectures.

The overwrought objection to this approach is that it will limit innovation and guide development down unfruitful paths. After all, that is the point of the washing machine story mentioned earlier. The problem is, while the anecdote is amusing, it does not reflect how modern washing machines were developed. Engineers at Maytag did not begin by articulating abstract requirements for the removal of particulate matter greater than  $n$  microns in size from fabrics composed of cotton fibers, to an effective level of only  $k$  residual particles per gram of fabric after  $t$  seconds of processing. Rather, history shows an incremental progression of machines

which largely draw from automation of (formerly) human actions, but with innovative progressions.

Developers, nonetheless, do have to be concerned about having their vision limited by current designs. An analogy used by Garlan and Shaw makes the point well: to ascend to the top of a house a ladder may be used. To ascend to the top of a small building, a fire truck ladder may be used. But to ascend to the top of a skyscraper a ladder of any variety will be insufficient; an elevator (which bears no physical relationship to a ladder) is effective. To ascend to the moon yet another totally different technology is required. In this analogy the concept of “ascension” is constant across the different situations, but the specifics of the situations end up implying the need for distinctly different solutions (“architectures”).

The point is this: predecessors, i.e. existing architectures, provide the surest base for the *vast* majority of new developments; in such situations requirements should be stated using the terminology and structural concepts of existing systems. In situations where an adequate (“physical”) predecessor is *unknown*, conceptual predecessors or analogies (e.g. “things used before to ascend”) may provide a terminological basis for describing the new needs, but caution must be exercised in drawing any architectural notions from such predecessors. Conceptual predecessors may provide a vision but offer little help beyond that<sup>4</sup>.

Perhaps most dangerous is the so-called “greenfield” development: one in which there is no immediate architectural predecessor. In such cases the temptation is to believe that new conceptual ground is being broken and hence no effort need be or should be undertaken to examine existing systems and architectures for framing the requirements. The risk is a directionless development; better is the strategy to first extensively search for existing architectures which might provide the efficient basis for framing the new requirements and solution. Greenfields are often minefields in seductive disguise.

---

<sup>4</sup> Nonetheless the considerable inspiration that can come from considering an analogy from a different domain of knowledge should not be underestimated. An example *par excellence* is the invention of hypertext: Vannevar Bush in his article “As We May Think” [34] – Bush, V. As we may think. *interactions*. 3(2), p. 35-46, 1996. conceived of the notion of hypertext through explicit analogy to how the human brain operates associatively. His conception for a device for making and recalling information associatively, however, had nothing to do with biology or cells, but rather with extrapolations from mechanical devices of the 1940’s.

Lastly, the admonition to always consider architectural predecessors and to base development on improvements to existing systems is not absolute. Not all architectures are worthy of further work, and may be incapable of serving as the basis for additional development. As further chapters will illustrate, some architectural styles are much more effective at supporting change and enhancement than others. Some architectures deserve to be abandoned.

This section has called for a new understanding and approach towards requirements engineering which provides substantial prominence to the role of architectures and solution considerations. Architectures provide the language for discussion of needs – not only a glossary of terms, but a language of structures, mechanisms, and possibilities. With this architectural underpinning preliminary analyses can proceed.

Requirements documents still serve an important role in the engineering process, for instance as the basis for contracts and setting out the precise objectives for new work, but these documents should be strongly informed by architectural considerations. Chapter 15 will elaborate an advanced application of these ideas known as “reference requirements”, under the banner of “domain specific software architectures”. Later in this chapter we will briefly return to the relationship between requirements and development, when in the section on processes we consider the “Twin Peaks” model and “agile development methods”.

## 2.3 Design

Designing is, by definition, the activity that creates a system’s software architecture – its set of principal *design* decisions. As the preceding sections have indicated, these decisions are not confined, e.g., to high level notions of a system’s structure. Rather the decisions span issues that arise throughout the development process. Nonetheless there is a time during development when more attention is paid to making many of those principal decisions than at other times – an architectural design “phase”.

Our points for this section are simply as follows:

- The traditional design phase is not *exclusively* “the place or the time” when a system’s architecture is developed – for that happens over the course of development – but it is a time when particular emphasis is placed on architectural concerns;
- Since principal design decisions are made throughout development, designing must be seen as an aspect of many other development activities;
- Architectural decisions are of many different kinds, requiring a rich repertoire of design techniques.

In classical software engineering, the activity of design is confined to the “design phase”. In the notional waterfall model, the abstract requirements produced by the requirements phase are examined, some design process is followed, and at completion of the phase a design is produced and handed to programmers for implementation. Most often those decisions concern a system’s structure, including identification of its primary components and how they are connected. (Hence such a design denotes a particular set of design decisions that *partially* comprise the architecture.) To the extent that, during the design phase, some portion of the requirements are found to be infeasible, those requirements issues are referred back to the requirements “phase” for reconsideration (and, in the extreme purist view, without passing back any solution information!) If any portions of the design are found to be infeasible or undesirable during the implementation phase, those issues are referred back to the design “phase” for reconsideration.

With an architecture-centric approach to development these artificial and counterproductive phase boundaries are diminished or eliminated. As the previous section discussed, the analysis of requirements is properly bound up with notions of architecture and design, with these notions providing the context and vocabulary for describing the new capabilities desired. The activities of analysis, design, and implementation proceed, but in an enriched and more integrated fashion. The principal decisions governing an application – its architecture – are informed from many sources and typically made throughout the process of development.

Lastly, a rich repertoire of design techniques is needed to assist the architect in making the wide range of design decisions comprising an architecture. The architect must deal, for example, with

- stakeholder issues, such as choices concerning the use of proprietary, commercial off-the-shelf, or open-source components, with their attendant and varying licensing obligations;
- overarching style and structure;
- types of connectors for composing sub-elements;
- package and primary class structure (i.e., low-level style and structure when in an object-oriented development context);
- distributed and decentralized system concerns;
- deployment issues;
- security and other non-functional properties;
- post-implementation issues (means for supporting upgrade and adaptation).

Clearly, a simple one-size-fits-all design strategy will not suffice. The following subsection considers the topic of design techniques in a little more detail. In many ways, however, everything in the rest of this book is an exploration of the many facets of software design – this section provides only the briefest introduction.

### 2.3.1 Design techniques

A variety of strategies exist for helping the designer develop an architecture. Chapter 4 will discuss several of them in substantial detail, including the use of basic conceptual tools, architectural styles and patterns, and strategies for dealing with unprecedented systems. For the purposes of this chapter, namely relating an architecture-centric approach with classical software engineering, we only consider two strategies for use in development of a solution architecture: object-oriented design and the use of domain-specific architectures, just to illustrate the spectrum of approaches, issues, and concerns.

Object-oriented design is considered first, since it is perhaps the most common design approach taught, and also because close consideration of it helps reveal why a wide repertoire of techniques is necessary. A similar analysis could be developed for other traditional approaches to design, such as functional decomposition.

#### Object-oriented design

One strategy for development of a system's design that programmers are usually familiar with is object-oriented design (OOD). OOD is usually taught in the context of object-oriented programming, i.e. the reduction of an algorithm to machine-executable form. The essence of OOD is the identification of so-called objects, which are encapsulations of state with functions for accessing and manipulating that state. Numerous variations are found in different object-oriented programming languages for the way objects are specified, related to one another, created, destroyed, and so on.

While object-oriented design can be used as a strategy when developing an architecture, it is not a complete approach, and is not effective in all situations. This is not to say that it is an ineffective design technique. On the contrary, OOD is exceptionally effective in a wide variety of development situations! It is just important to realize its limitations, so that other additional or alternative techniques can be brought to bear on those portions of the task.

First, clearly, OOD is not a complete design approach, for it fails to address a myriad of stakeholder concerns. OOD says nothing about deployment issues, security and trust, or use of commercial components, for instance. Similarly, OOD, as a practice, has no intrinsic means for carrying forward domain knowledge and solutions from previous architectures to new products. While code reuse techniques may be employed or higher level representations such as UML used, no facility is

available for explicitly indicating points of variation or other aspects of program families.

Second, OOD is not effective in all situations. For instance, some of its limitations are as follows.

- OOD views all applications as consisting of, solely, one software species (namely, "object"), regardless of purpose. Forcing all concepts and entities into a single mold can obfuscate important differences. The REST style, for instance, maintains distinct notions of "user agent", "origin server", and "cache". Apart from using programming language types to try to characterize these distinct elements, OOD does not offer any helpful modeling mechanism.
- It provides only one level of encapsulation (the object), one notion of interface, one type of explicit connector (procedure call), no real notion of structure (objects are constantly created and destroyed), and no notion of required interfaces. This implies that all the richness of a given solution approach has to be mapped down or transformed to this level of single "choice". Some architectures – such as pipe and filter – may not be at all effective after such a transformation.
- OOD is so closely related to programming language concerns and choices that it tends to have the forest obscured by the trees. For instance, the vagaries of type inheritance may obscure identification of the principal objects critical to the design. Similarly it is so bound with programming language issues that the language may start dictating what the important decisions are.
- The typical OOD approach assumes a shared address space and adequate support for heap and stack management. OOD assumes a single thread of control; support for multiple threads is accommodated in languages largely as an afterthought. Concern for concurrent, distributed, or decentralized architectures is largely outside the OOD purview. Support for distributed objects, such as that provided by CORBA-style middleware, attempts to hide the presence of network boundaries. Architectures that must deal with the realities of networks and their unavoidable characteristics of introducing failures, latency, and authority domains will not be directly supportable with an OOD approach.

One positive step in the object-oriented design world has been the creation of the UML modeling notation. This has helped lift the discussion of object-oriented designs above the programming language level. In 2003 the UML notation was enhanced with some simple notions of software architecture, further improving its contribution. UML is covered later in this text, in Chapters 6 and 16.

Also helping to lift object-oriented design closer to a richer notion of architecture is the extensive work in patterns, as exemplified in the work of Gamma, Helm, Johnson, and Vlissides [85]. Patterns are explicitly designed to enable the carry forward of knowledge and experience from previous work into new applications. As such, patterns represent an excellent, "in the small," OO-particular application of an important concept from software architecture.

Extending the idea of patterns to a broad, application-encompassing level yields a design approach known as domain-specific software architectures. This approach exemplifies how architecture-centric design may be supported, and how significant technical and business benefits can consequently be achieved.

#### **Domain-specific software architectures (DSSAs)**

The approach known as "domain specific software architectures," or DSSAs, is appropriate when prior experience and prior architectures are able to strongly influence new projects. The key notion is that if a developer or company has worked within a particular application domain for many years, it is likely that a "best approach" or "best general solution" for applications within that domain will have been identified. Future applications in that domain can leverage this knowledge, with those applications having their fundamental architecture determined by the architectures of the past generations of applications. Indeed, the new architectures will likely be variations on the previous applications. The technical essence of the DSSA approach is to capture and characterize the best solutions and best practices from past projects within a domain in such a way that production of new applications can focus more-or-less exclusively on the points of novel variation. For those points where commonality with past systems is present, reuse of those corresponding parts of the architecture, and indeed reuse of corresponding parts of the implementation, is done. The DSSA approach to system development is thus consistent with the development of product lines, and can be the key technical element in a product line approach.

For instance, if a company is in the business of producing television sets for the world market, such as the example of Philips discussed in Chapter 1, a "backbone" software architecture can be identified that can be used in TVs destined for sale in North America, Europe, and the Far East. Different tuners for the different markets can be written, and if the backbone architecture has identified variation points and interfaces for the tuner component, the various market-specific tuners can be slotted in, enabling customization in a very cost effective manner.

To effectively follow the DSSA approach some good technical support is required: the architecture of the previous generation of applications must

be captured, the points of allowable variation identified and isolated, the interfaces between the points of variation and the "core" architecture explicit, the dependencies between multiple points of variation identified, and so on. These issues and more are explained in Chapter 15, where the DSSA concept and product lines are explored in depth. Suffice it to say here that the DSSA approach to design enables the many advantages of an architecture-centric development approach to be realized.

## **2.4 Implementation**

The task of the implementation activity is to create machine-executable source code that is faithful to the architecture and which fully develops all outstanding details of the application. This is true whether speaking from the perspective of classical software engineering or from the software architecture-centric view of software engineering set forth in this book.

Architecture-centric development somewhat changes the responsibilities of the implementation activity, however, and emphasizes some particular approaches to implementation. Specifically, the architecture approach emphasizes keeping all the recorded decisions constituting the architecture consistent with the code as the application is fully elaborated. That is, the implementation activity cannot turn its back upon the preceding decisions and proceed to modify the application's structure without making corresponding changes to the recorded architecture. With regard to implementation strategies, architecture-based development recognizes the enormous cost and quality benefits that accrue from generative and reuse-based implementation strategies. In those cases where full automatic generation is not possible, a set of supportive techniques are emphasized, such as application frameworks and other types of code reuse, which provide significant parts of the implementation pre-built.

The watchword for the creation of the implementation is its being "faithful" to, or consistent with, the architecture. The simplest understanding of a faithful implementation is that all of the structural elements found in the architecture are implemented in the source code, and that all of the source code corresponds to various parts of the explicit architecture. It is fair for the source code to contain more details, such as low-level algorithms for implementing a higher level concept described in the architecture, but the source code must:

- not utilize major new computational elements that have no corresponding elements in the architecture;
- not contain new connections between elements of the architecture that are not found in the architecture (e.g. such as might be motivated by efficiency concerns).

This initial conception of the relationship between the architecture and the source code is not fully adequate, however, for it does not accommodate some of the characteristics of reuse-oriented engineering. For instance, an architecture may require the presence of a component to perform some mathematical functions – a sine and cosine routine perhaps. The most cost-effective and quality-focused approach to providing an implementation for that component may be to acquire and use a general math library, one providing not only sine and cosine functions, but tangent, inverse trig functions, and so on. Such a component may have interfaces in addition to those required by the architecture, and will certainly contain sub-functions that do not correspond to anything identified in the architecture specification.

Further issues may come into this notion of faithfulness between the implementation and the architecture as it existed before the implementation began. Examination of a candidate mathematics library may reveal that it provides 98% of the functionality required by the architecture, for a very low price, and at a very high quality level. Analysis of the consequences of the missing 2% of the functionality may lead the designers to conclude that the missing functionality will be acceptable under most usage situations, and for the cost savings realized, (1) choose to use the library and (2) revise the specifications of the system, including the architecture, in accordance with the reduced functionality. The critical point is that the architecture is always kept in a consistent state with the implementation.

#### 2.4.1 Implementation strategies

A variety of techniques are available to assist in the faithful development of the implementation from the design, including generation technologies, frameworks and middleware, and reuse. Choice of the techniques is largely determined by availability. Generative techniques, when available, are often the best: the implementation is generated automatically and is of very high quality. The reuse-based techniques come next: implementation time is significantly less than programming the entire implementation from scratch and quality is similarly better. Least desirable is writing all the code manually: the project cost goes up significantly due to extended development and quality assurance time. These various approaches are discussed below.

The use of generation technologies is the easiest and most straightforward way of ensuring complete consistency between the architecture and the implementation. The concept is simple: for some application domains sufficient intelligence can be encoded in a tool such that a formal specification of the architecture can be input to the tool, and the tool will generate a complete program to perform the functions as specified. One

example of such technology is parser generators. Given the specification of the syntax of a programming language, a parser generator will generate a program capable of recognizing programs written in the language specified by the grammar. Choice of the parser generator determines the required form of the language specification and determines the structure of the generated parser, such as recursive descent or SLR(1)<sup>5</sup>. Generative techniques will be considered in much more depth in Chapter 9 (as will the other implementation technologies discussed below.)

The great attraction of generative technologies is, of course, that no human labor need be spent on programming. The limitation of the technique is just as obvious: the approach is only applicable in those limited situations where the domain is so thoroughly understood and bounded that generation is feasible.

For domains which do not satisfy the rigorous requirements of generative technologies, an effective approach is the use of “frameworks”. Frameworks are collections of source code with identified places where the engineer must “fill in the blanks”. That is, frameworks are defined in advance to implement portions of particular types or styles of architectures. The frameworks may be extensive, requiring only minor portions to be completed by hand, or may be very basic, only offering help in implementing the most generic aspects of an architecture or architectural style. In any case the places where the hand work must be done are defined in advance. The developer need not, indeed must not, stray from doing work only in those locations, and must do the work in those locations in such a way that it does not violate the design of the framework or of the architecture.

The role of frameworks in the implementation of an architecture is placed in context in Figure 2-1. Framework selection and development is an integral part of architecture-based system implementation, because the framework provides the bridge between concepts from the architecture and concepts from the platform (i.e., programming language and operating system). If a framework does not exist for a particular combination of architecture and platform, conscientious developers will generally end up implementing one anyway because of the general software engineering principles of abstraction and modularity—frameworks encapsulate key features necessary to map architectures to implementations.

<sup>5</sup> For a list of such tools, consult  
<http://www.thefreecountry.com/programming/compilerconstruction.shtml>

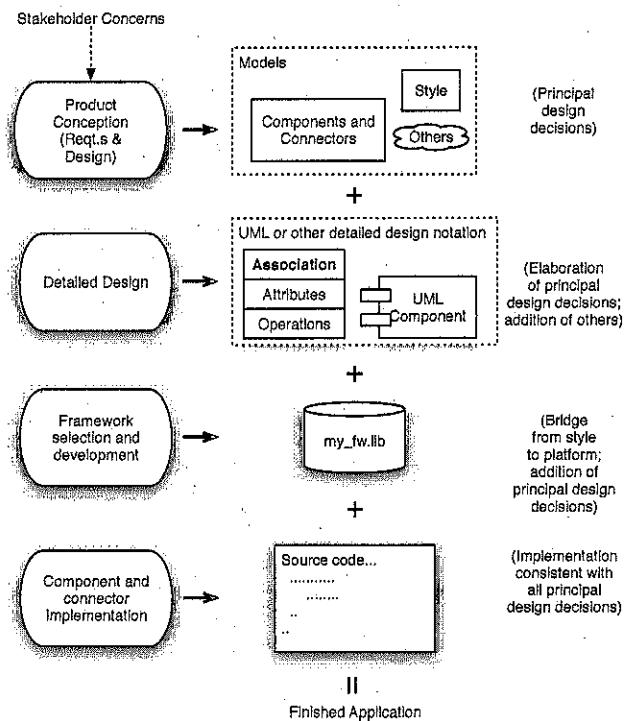


Figure 2-1.  
Frameworks and the  
Implementation activity  
in the context of  
development. Activities  
are shown in the  
leftmost column;  
artifacts are in the  
central column;  
notes are on the right.

Common frameworks in extensive use are those targeted at supporting implementation of user interfaces. Both the Microsoft Foundation Classes (MFC) and the Java Swing library represent frameworks that provide the user with common user interface widgets and interaction methods in object-oriented libraries. More than simply providing a set of facilities that users can take advantage of, these frameworks fundamentally influence the architectures of systems that employ them. For example, both frameworks (to some degree) manage concurrency and threading—the frameworks themselves create and manage the threads of control responsible for gathering user input events from the operating system and dispatching them to processing code developed by the user.

Related to frameworks, as aids for assisting in the implementation of architectures, are middleware technologies. Middleware comes in several

varieties, some of which provide an extensive range of services, but as a whole they typically support communication between software components. As such, middleware facilitates the implementation of connectors—the architectural elements responsible for providing communication between components. The developer has complete responsibility for implementing an architecture's components' business logic, but relies on middleware for implementation of connectors.

Commonly found middleware includes CORBA and Microsoft's DCOM (for supporting communication between remote objects), RPC (for remote procedure calls), and message-oriented middleware (for delivery of asynchronous messages between remote components).

Generative technologies, frameworks, and middleware thus represent a spectrum of generic and widely used technologies for assisting in the faithful implementation of an architecture. These technologies progress from fully automatic, to partially automatic (filling in the blanks in frameworks), to providing help with the implementation of connectors (middleware).

Less generic, but no less important, is the reuse of software components, whether commercial off-the-shelf, open-source, or in-house proprietary software. The key issue of such reuse, as it pertains to the faithful implementation of an architecture, is the degree to which the functionality, interfaces, and non-functional properties of a candidate component for reuse match those required by an architecture. In the (unfortunately) unlikely event that a perfect match exists, the job is done. In the common case, namely some degree of mismatch, the issues and choices are difficult. One strategy, which preserves the architecture as specified, is to encapsulate the pre-existing component inside a new interface so that the thus-modified component exactly meets the requirements of the architecture. While this technique can be successful, a more likely circumstance is that performing such encapsulation will still not be economically or technically viable. In such cases a decision needs to be made: whether to revise the architecture in such a way as to enable the reuse of the component, or to abandon this particular pre-existing code and either search for alternatives or create a new component from scratch. This choice is a difficult one.

In absence of any technology to assist the developer in creating source code faithful to the architecture, the implementation must be developed manually. In such circumstances the programmer must rely upon discipline and great care, for this can be the “great divide.” To the extent that the implementation differs from the architecture which resulted from preceding development activities, that “architecture” does not characterize the application. The implementation *does* have an architecture: it is

latent, as opposed to what is documented. Failure to recognize this distinction:

- robs one of the ability to reason about the application's architecture in the future;
- misleads all stakeholders regarding what they believe they have as opposed to what they really have;
- makes any development or evolution strategy that is based on the documented (but inaccurate) architecture doomed to failure.

Chapter 9 takes up these various issues in detail.

## 2.5 Analysis and Testing

Analysis and testing are activities undertaken to assess the qualities of an artifact. In the traditional waterfall, analysis and testing are conducted after the code has been written, in the “testing phase”. In this context the artifact being examined is the code; usually the quality being assessed is functional correctness, through properties such as performance may be examined as well. Analysis and testing activities do not have to be confined to occur after programming, of course, and many excellent development processes integrate these activities with the development process. As long as an artifact exists which is susceptible to analysis for a defined property, that analysis can proceed – whether the artifact is a requirements document, or a description of the application’s structure, or something else. One of the virtues of conducting analysis before code exists is cost savings: the earlier an error is detected and corrected the lower the aggregate cost.

Given that early detection of errors is a good thing, one must ask why conventional analysis and testing is almost always confined to simply testing source code. Moreover, why is such testing performed only against the most basic of specifications, namely the system functional requirements? The answer is almost always because of the non-existence of any sufficiently rigorous representation of an application apart from source code. Rigorous representations are required so that precise questions can be asked and so that definitive answers can be obtained – hopefully by means of automated analysis aids.

A technically-based, architecture-centric approach to software development offers significant opportunity for early analysis and for improved analysis of source code. Additionally, the prospect for analyzing properties other than just functional correctness is present. In this approach to development, technically-rich architectural models are present long before source code, and hence serve as the basis for and subject of early analysis. Chapter 8 will present substantial details on

architectural analysis, Chapter 12 will extend that discussion to non-functional properties, and Chapter 13 will delve in particular to architectural support for security and trustworthiness. In the few paragraphs below we simply outline some of the approaches; details will have to wait until after our presentation of architectures and architectural models is on a more precise footing.

First, the structural architecture of an application can be examined for consistency, correctness, and exhibition of desired non-functional properties. If the architecture upon which the implementation is (later) based is of high-quality, the prospects for a high-quality implementation are significantly raised.

As a formal artifact, the architectural model can be examined for internal consistency and correctness: syntactic checks of the model can identify, for instance, mismatched components, incomplete specification of properties, and undesired communication patterns. Data flow analysis can be applied to determine definition/use mismatches, similarly to how such analysis is performed on source code. More significantly, flow analysis can be used to detect security flaws. Model checking techniques can analyze for problems with deadlock. Estimates of the size of the final application can be based upon analysis of the architecture. Simulation techniques can be applied to perform some simple forms of dynamic analysis.

Second, the architectural model may be examined for consistency with requirements. Regardless of whether the requirements were developed in the classical way (i.e. before any development of solution notions), or in the modern sense, in which the two are developed in concert, the two must be consistent. Such examination may be limited to manually-performed analysis if the requirements are stated in natural language. Nevertheless such comparisons are essential in guaranteeing that the two specifications are in agreement.

Third, the architectural model may be used in determining and supporting analysis and testing strategies applied to the source code. The architecture, of course, provides the specifications for the source code, so consistency between them is essential, as we discussed earlier in this chapter. Concretely, as the specification for the implementation, the architecture serves as the source of information for governing specification-based testing at all levels: unit, sub-system, and system level.

The architecture can prioritize analysis and testing activities, and focus those activities on the most critical components and sub-assemblies. For example, in the development of a family of software products, special attention should be paid to those components which are part of every

member of the product family: an error in one of them will affect all the products. Conversely, a component which only implements a rarely used and non-critical feature of one member of the family may be judged to not merit nearly as much scrutiny. Testing costs money, and organizations must have a means for determining the priorities for their testing budget; architecture can provide some of that guidance.

In a similar vein, architecture provides a means for carrying forward analysis results from previous testing activities, with accompanying cost savings. For instance, if a particular component is reused in a new architecture, the degree of its unit testing can be reduced if examination of the architecture confirms that the context and conditions of use are the same (or more constrained) than the earlier use.

Architecture can provide guidance and economies in the development of test harnesses. (Test harnesses are small programs used to test components and sub-assemblies of larger applications. They provide the analyst with the ability to conveniently and effectively test the “internal parts” of an application. It can be difficult, for instance, to use system-level inputs to fully and economically exercise the boundary conditions of an internal component.) For instance, if an architecture is designed to support a product family, and a small set of components are changed to customize the product for a particular market, a test harness can be constructed to focus testing on those components that comprise the change set. Each customized product can thus have a testing regimen emphasizing only those parts which have changed.

Architecture can also provide guidance in directing the analyst’s attention to the connectors in a system’s implementation. As will be discussed in Chapter 5, connectors play a particularly important role in some systems’ structure, being tasked with supporting all inter-component communication. The architecture provides an effective way for identifying those points of special leverage, and hence can aid in shaping the analysis and testing activity. Additionally, some connectors offer particularly effective opportunities for non-intrusive monitoring and logging of applications, which can play a key role in helping an engineer develop an understanding of how a system works, as well as assisting in analysis and testing.

Fourth, the architectural model can be compared to a model derived from the source code of an application. This is a form of “checking your answer”. Stated abstractly, suppose program P is derived from architecture A. A separate team of engineers, with no access to A, could, by reading and analyzing P, develop an architectural model A’ – a model of the architecture that P implements. If all is well, A will be consistent with A’. If not, either P does not faithfully implement A, or else A’ does

not faithfully reflect the architecture of P. Either way, an important inconsistency can be detected.

This abstract characterization is not very practical, as it would likely involve substantial human labor. But particular features of implementations can be readily extracted and compared with the architecture. For instance, it is straightforward to extract a model from source code that shows which components communicate with which others. That communication pattern can be compared to the corresponding communication pattern in the architecture and any discrepancies noted. An example of this type of analysis appears in the following chapter.

As noted above, substantive consideration of the analysis of architectures must wait until later in this text. Techniques for representing architectures must first be presented (see Chapter 6). It is sufficient for now to note that architecture-centric development provides a variety of new and significant opportunities for assessing and hence improving the quality of systems.

## 2.6 Evolution and Maintenance

Software evolution and software “maintenance” – the terms are synonymous – refer to all manner of activities which chronologically follow the release of an application. These range from bug fixes to major additions of new functionality to creation of specialized versions of the application for specific markets or platforms.

The typical software engineering approach to maintenance is largely *ad hoc*. In a “best practices” situation, each type of change causes the software process to return to whatever phase that issue is normally considered in, and the development process restarts from that point. Thus if new functionality is requested, that requires returning to the requirements analysis phase and then moving forward in sequence from there. If the change is thought to be a minor bug fix, then perhaps only the coding phase and its successors are revisited.

The major risk presented by evolution is degradation of the quality of the application. Intellectual control of the application may degrade if changes may be made anywhere, by whatever means are most expedient. In practice, this is precisely what happens. Rather than following “best practices,” it is common for only the coding phase to be revisited. The code is modified in whatever way is easiest. Over time the quality of the application degrades significantly, and making successive changes becomes increasingly difficult as complex dependencies between ill-considered earlier changes come to light.

An architecture-centric approach to development offers a solid basis for effective evolution. The key is a sustained focus on an explicit, substantive, modifiable, faithful architectural model.

The evolution process can be understood as consisting of the following stages:

- o motivation,
- o evaluation or assessment,
- o design and choice of approach,
- o action, which includes preparation for the next round of adaptation.

The motivations for evolution are many, as noted above. We draw special attention to the creation of new versions of a product. This motivation does not often appear in traditional treatments of software evolution, but is common in the commercial software industry. This kind of change raises the topic of software product families, and as discussed in Chapter 1, supporting product families can be a particular strength of architecture-centric approaches.

Whatever the motivation for evolution may be, the next step is assessment. The proposed change, as well as the existing application, must be examined to determine, for example, whether the desired change can be achieved and, if so, how. Put another way, this stage requires deep understanding of the existing product.

It is at this point that the architecture-centric approach emerges as a superior engineering strategy. If an explicit architectural model that is faithful to the implementation is available, then understanding and analysis can proceed efficiently. A good architectural model offers the basis for maintaining intellectual control of the application. If no architectural model is available, or if the model in existence is not consistent with the implementation, then the activity of understanding the application must proceed in a reverse-engineering fashion. That is, understanding the application will require examination of the source code and recovery of a model which provides adequate intellectual basis for determining how the needed changes can be made. This is time-consuming and costly, especially when the personnel involved are new to the project.

Errors in maintenance often arise from shortchanging this activity. If there is insufficient understanding of the existing structure, then plans to modify that structure will likely fail – at the points of misunderstanding.

In contrast, a good architectural model offers a principled basis for deciding whether a desired modification is reasonable. A proposed change may be found to be too costly or detrimental to system properties

to warrant development. Only with a good intellectual grip on the existing architecture, as well as the proposed change, can such a determination sensibly be made. The net effect of this principled approach will be the maintenance of architectural integrity and the attenuation of requirements volatility.

The next stage in evolution is development of an approach to satisfy whatever requirement motivated the activity. Likely several courses of action will be identified, so a further step of choosing among alternatives is required.

Once a course of action is determined, it must be put into action. For changes of even moderate significance the first artifact to be modified should be the model of the architecture. In particular, if the change needed pertains to the architecture, then changing the architecture is the place to begin. After changing the architecture corresponding changes to code can be made. The critical matter, of course, is maintaining consistency between the architecture and the implementation, as discussed earlier in this chapter. Tools can help with this task.

A mistake to avoid is changing the code first and then “planning to” revise the architectural description to match. Following up afterwards on that good intention seldom takes place.

Making the various changes needed to accommodate whatever motivated the evolution activity should not be considered complete until all elements of an application – architecture and code – are consistent. The reason is simple: additional needs for evolution will be identified in the future. If the application is left inconsistent it will sabotage those future evolution activities.

In conclusion, software will evolve, whether one is using an architecture-centric development process or not. The question is whether or not such evolution will proceed efficiently and whether it will result in the degradation of the quality and intellectual integrity of the product. Architecture provides the bedrock for maintenance of coherence, quality, and control. These issues are discussed in greater detail in Chapter 14.

## 2.7 Processes

A key theme of this chapter has been that architecture concerns properly permeate the entire software development and evolution activity. The set of decisions comprising the architecture forms in concert with the requirements and continues to expand through maintenance. The architecture is thus under constant change.

Architecture, correspondingly, is not a "phase" in a software engineering process; it is a core, evolving body of information. Indeed, the development of this body of information may reach back and out to preceding applications and other applications.

The centrality of architecture to software development, and the insights that arise from a focus on architecture, are unfortunately totally obscured in traditional characterizations of the software development activity. Traditional software process discussions makes the process activities the focal point; the architecture (and hence the product!) is often nowhere to be found. Equally bad, the standard software development processes encourage, if not enforce, sharp divisions between various types of development activities. For instance the waterfall and spiral models both separate the activity of requirements determination from the activity of design development. As we have seen, such boundaries are not warranted and indeed are counterproductive.

Simply stating, however, that software development processes should be architecture-centric does not by any means say that there is a single "right" way to proceed in application development. Different organizations and engineers will wish to adopt particular strategies to best take advantage of their particular organizational strengths and preferences. Equally important, different development settings (e.g., knowledge, pre-existing developments, component libraries, codified architectures) will demand that different prominence be given to the various types of development activities, and those activities will vary in the amount of time required for their completion.

Comparing, or even understanding, different strategies for software development requires a means for describing those strategies. A good descriptive formalism for characterizing strategies will provide a way of not only showing what activities are occurring when, but will give appropriate and effective prominence to the central role of architecture (and all other project artifacts) in the formation of the software product. Accordingly, we now present the *turbine model of software development*, and use it to characterize a variety of development strategies.

### 2.7.1 The Turbine Model

The turbine model is a means for describing and visualizing an integrated set of software development activities in which the central role of software architecture in the evolution of the product is prominently depicted. The model accounts for the following independent aspects of software development:

- o time
- o kinds of activities active at any given time

- o effort (e.g. labor hours expended) at any given time
- o product state (e.g., total content of product development, or knowledge, at any given time)

The model also shows a variety of combined factors, such as investment (cumulative effort over time-demarcated phases).

Viewed spatially, the model consists of a set of variable-width, variable-thickness rings stacked around a core. The axis of the core is time; the core represents the software product (the architecture plus all the other artifacts comprising the product); the rings represent time-demarcated phases of development or evolution.

The simple, unidirectional waterfall is as simple in the three-dimensional turbine model as it is in its traditional depiction – save that the role of the software product is now evident. A nominal waterfall process is shown in three-dimensional perspective in Figure 2-2. An annotated side view of the same process is illustrated in Figure 2-3.

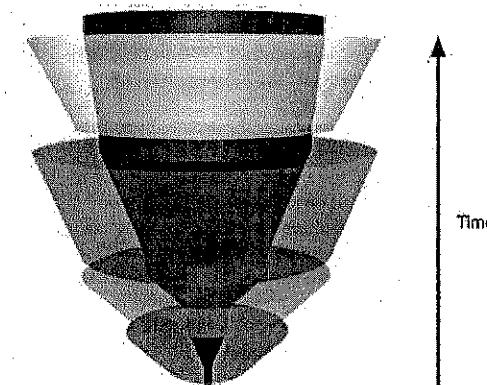


Figure 2-2. The unidirectional waterfall model as depicted by the turbine model.

Waterfall Example  
Angled Perspective

The first (i.e., bottom) ring of the example "waterfall turbine" begins with a null core, consists solely of the "requirements analysis" activity, and finishes at  $t_1$  with a core consisting solely of the requirements document. The second ring begins at  $t_2$ , consists solely of the design activity, and completes at  $t_3$ , with the core now consisting of both the requirements

document (unchanged since  $t_1$ ) and the design document. The third ring consists solely of the coding activity, and the fourth solely of the testing activity. Each ring adds one more element to the core. The added value of the turbine model is that, by portraying the growing core, the set of existing product elements is made clear. The testing phase, for instance, visibly has reference to not only the subject of the tests (the code) but the requirements that the code is supposed to satisfy – including any acceptance tests developed during the requirements phase.

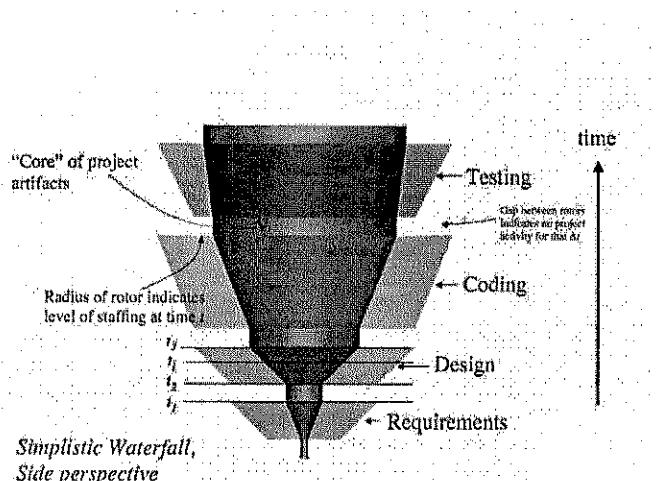


Figure 2-3. Side view, annotated, of the process depicted in Figure 2-2

A cross-section shows the state of the project at a given point in time. The area of the ring is proportional to the number of labor hours currently being invested in the project. The area of the core indicates the content of the product at that same time. Subregions of the core show the relative development of different parts of the product. An example is shown in Figure 2-4, at time  $t_1$  from Figure 2-3. The only activity is “Design” and the core consists of only the two documents shown.

### Cross-section at time $t_1$

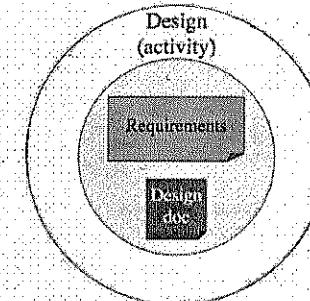


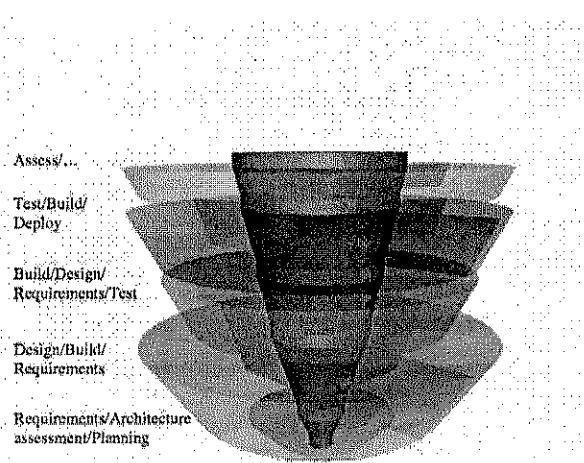
Figure 2-4. Cross-section of turbine from Figure 2-3 at time  $t_1$

The thickness of a ring denotes the time period during which the (possibly multiple, concurrent) activities of that ring are active, i.e. its duration. Consequently the volume of a ring (thickness \* area) represents the investment made during that ring: the product of the time that ring was active and the investment made during that ring. (Rings do not need to have the same cross-sectional area at  $t_i$  as they do at time  $t_{i+1}$ , but we will make that simplifying assumption for the moment.)

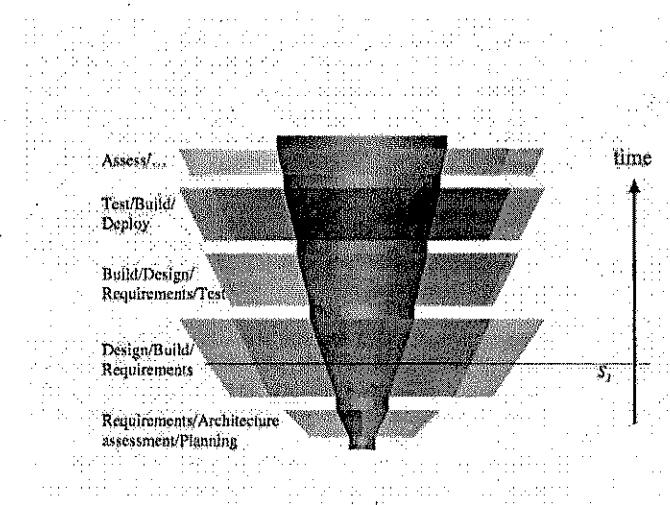
Since not all projects proceed in an uninterrupted fashion, gaps between rings represent periods of inactivity in a project. During such gaps the core is nominally constant – though if project data gets lost, the core would shrink correspondingly.

Rings may be divided into sub-areas, each of which represents a type of activity going on at that time. The activities shown in the sub-areas are *concurrent*. The relative size of the sub-areas denotes the share of the labor directed at that type of activity at that particular point in time.

A more complicated and much more realistic illustration that involves multiple concurrent activities is shown in Figure 2-5; a side view for this nominal project is shown in Figure 2-6.



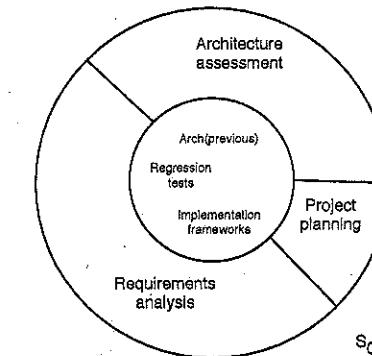
**Figure 2-5.** Example turbine model, shown in a 3-D perspective view, with rings color-shaded by type of activity. Transparency is used to enable seeing activities otherwise obscured.



**Figure 2-6.** Side view of the project shown in Figure 2-5

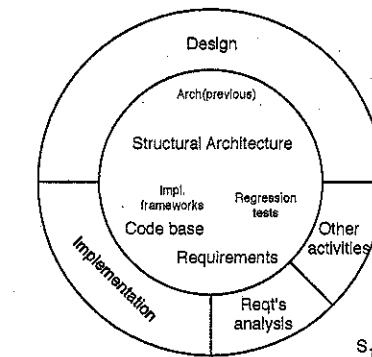
Cross-section  $S_0$ , shown in Figure 2-7, represents the state of the project at its beginning. The diameter of the core of the project is significant,

representing substantial knowledge and resources carried forward from previous projects. The activities at time  $t_0$  include architecture assessment (i.e. evaluation of architectures from previous projects), requirements analysis, and project planning.



**Figure 2-7.** Cross-section of turbine at time  $t_0$

Cross-section  $S_1$ , shown in Figure 2-8, represents the state of the project at time  $t_1$ . The core of the project has grown significantly, and particular sub-elements of the core are shown. The relative mix of the activities at  $t_1$  has changed also: a preponderance of the activity is devoted to design of the application's structure. A small amount of requirements analysis is still active, and some implementation is underway.



**Figure 2-8.** Cross-section of turbine at time  $t_1$

Cross-section  $S_n$ , shown in Figure 2-9, represents the state of the project near the time of its formal conclusion: the core shows a robust architecture, implementation, deployment processes, testing scripts, test results, and so on. The activity level is low, with remaining activities focused on capturing lessons learned.

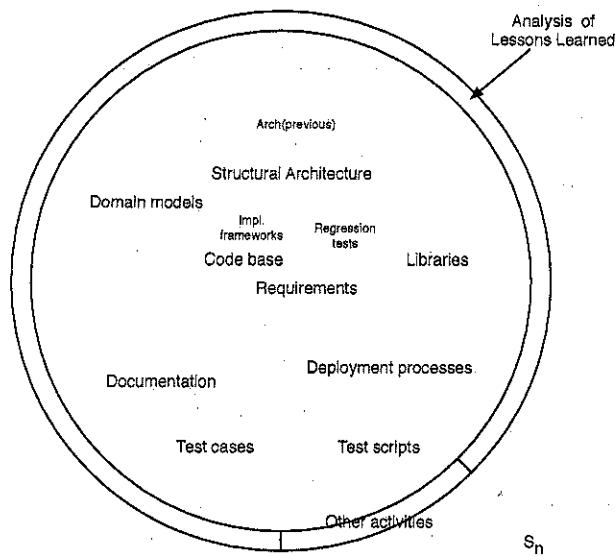


Figure 2-9. Cross-section of turbine at time  $t_n$

Viewed as a whole (Figure 2-5) it is evident that the purpose of the rings is to build the core. In other words, the purpose of the development activities is to create the product, in all its various details. These details and structures are abundant at the end of the development activities. This also highlights how a wise organization must treat this core: it is a composite asset of considerable size and value, and should be managed, post-project, accordingly.

Before going on, a few comments on the analogy used in naming the model/visualization are in order. Turbines are, of course, the engines that propel aircraft, generate hydroelectricity, and power a myriad other devices. The core of such turbines is the fluid that flows through them. With jet turbines the fluid is air; the "rings" of a jet turbine include the

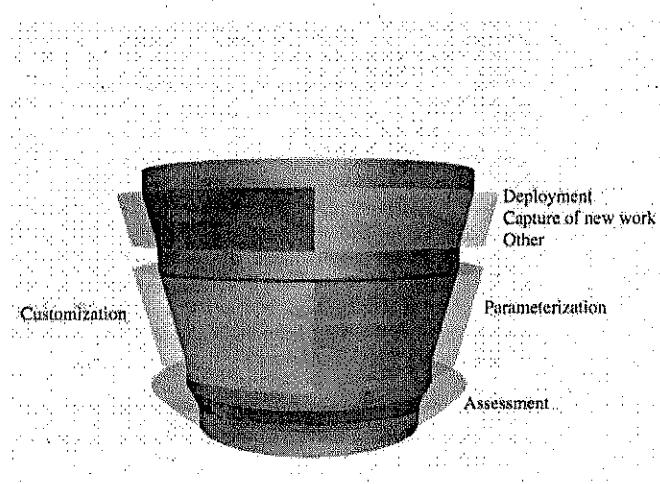
compressors with their fan blades whose job it is to compress the air, pushing it into the combustion chamber, where fuel is added and ignited. Other "rings" behind the combustion chamber contribute to the overall process, in which the air, now in large volume and at high speed, exits the engine. The analogy to software development is only a mild one and should not be pressed very far. But the product is the focus of the turbine; each ring and element contributes to that product. The air flows through the turbine, and is touched by each of the various rings. So, too, does the software product, and the architecture in particular, represent the core of software development. It is touched and (hopefully) enhanced by each aspect of software development. In contrast to a physical turbine, however, each ring of software development genuinely adds to the core, not merely just heating it up. (Other difficulties – or "advantages" – of the analogy, such as the rings spinning in circles and the product just being hot air, are strictly unauthorized!)

Two further examples are shown now, where use of the turbine model highlights distinctive aspects of these approaches to software development.

#### A Robust Domain-Specific Software Architecture-based Project

Figure 2-10 shows a turbine model visualization of a notional project that was based upon a pre-existing domain-specific software architecture, i.e., a project similar to the Philips television example of Chapter 1. At the project outset the core is quite large: it contains a multitude of reusable artifacts from preceding projects. The activities are thus (1) to assess these artifacts to ensure that the current project fits within the constraints imposed by those artifacts, (2) to parameterize those artifacts to meet the new project's needs and to perform any customization necessary, and (3) to integrate, assess, and deploy the product.

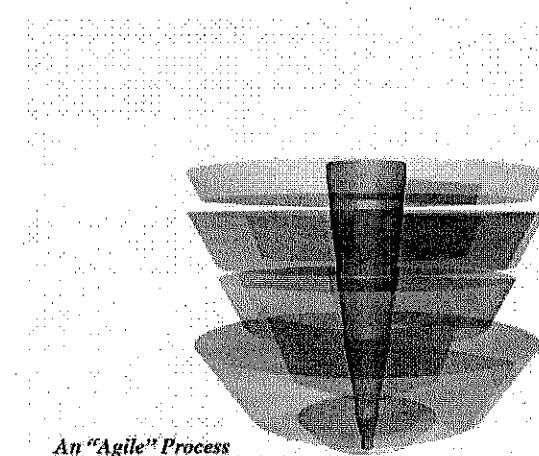
**Figure 2-10.** A development process based on an existing domain-specific software architecture and reuse library.



#### Agile Development

The turbine model can be used in analyzing alternative approaches to software development. For example, Figure 2-11 shows a notional “agile” development process. Agile processes are positive in showing, and emphasizing, concurrency between a variety of kinds of development activities: requirements elicitation and development of tests, for instance. As the development progresses those activities do not cease, e.g., once code development is begun. Indeed all these activities continue throughout the project.

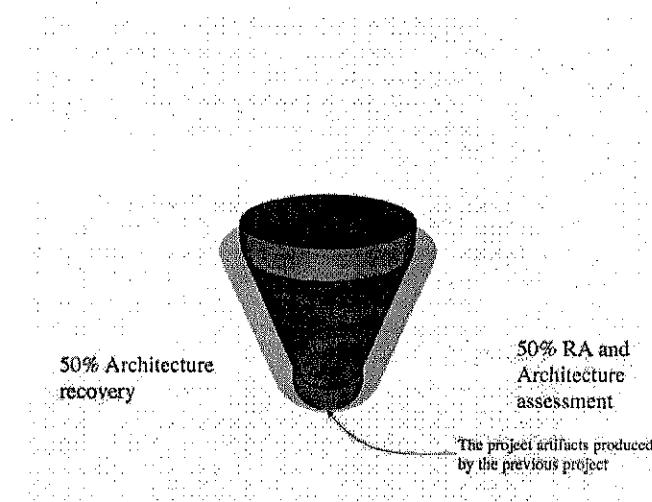
**Figure 2-11.** Turbine model of a notional agile development process.



As the “skinny core” of the turbine model indicates, however, the agile process denies development of any explicit architecture; rather for the “agile developer” the code *is* the architecture. The visualization indicates that the agile process starts with a core that is devoid of any architecture and terminates similarly. A large body of code may be present, along with, perhaps, requirements documents or user guides, but no explicit record of the fundamental design decisions, such as the application’s architectural style.

The problems with this approach are made clear when a follow-on project is required. That is, if at some point after the first agile project completes its development, a follow-on project is required to have the application meet some new demand. Unless the same development team – with excellent memories – is employed on the subsequent project, an initial project model such as shown in Figure 2-12 may be anticipated. In particular a significant ring of activity will be required at the beginning of the project to simply understand the existing code base and recover the latent architecture so that planning for how to meet the new needs can proceed.

**Figure 2-12.** Initial portion of a turbine model of a “phase 2” agile process.

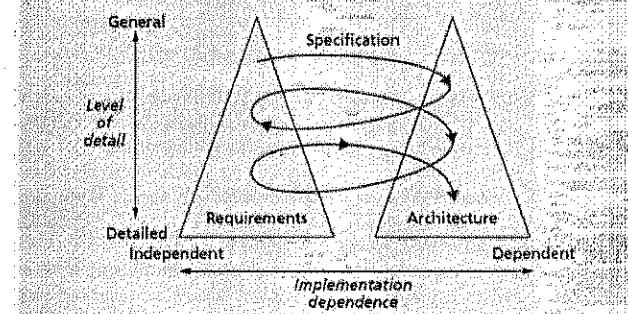


#### Other Processes and Process Models

A variety of researchers and organizations have promulgated processes that, to a greater or lesser extent, show the special role of architecture in development. One of the best of these is the “Twin Peaks” model, of Nusibeh. Twin Peaks emphasizes the co-development of requirements and architectures, incrementally elaborating details. The model is illustrated in Figure 2-13, which is taken from the Twin Peaks paper.

**Figure 2-13.** Twin Peaks model of development.

N.B. Need the appropriate permissions to reuse this figure.



**Figure 1.** The Twin Peaks model develops progressively more detailed requirements and architectural specifications concurrently. This is an adaptation of the model first published in Paul Ward and Stephen Mellor’s Structured Development for Real-Time Systems: Introduction and Tools, vol. 1, Prentice Hall, Upper Saddle River, N.J., 1985, and subsequently adapted by Andrew Vickers in his student lecture notes at the University of York, UK.

It is left as an exercise for the reader to create a turbine model visualization of the Twin Peaks process shown in the figure. It should also be noted that the Twin Peaks work is representative of recent work in requirements engineering which is now giving much more prominence to the role of design and existing architectures in the activity of product conception.

#### Brooks’ Law and Software Architecture:

“Brooks’ law: Adding people to a late software project makes it later.”

This adage is one of the best known in software engineering. Yet the reasons why it is so often true are seldom explained. Fred Brooks gave those reasons in an interview: “Brooks’ law depends heavily on the amount of information that has to be communicated. So the argument is that if you add people to a project that you already know is late, which means you’re at least in the middle of the project, you have to repartition the work. That’s a job in itself. Just deciding who is going to do what means that instead of having the thing divided into the units you had it divided into, you have to divide it into more units. Sometimes that can be done by subdividing the existing units, but sometimes you have to move boundaries. That’s a lot of work. The next thing is, you have to train the new people. Who can train them? Only the old people. So they quit working and go to training. And the new people are green and have to get up to speed. So there’s a period where they’re unproductive, and there’s a

period when they are less productive. And there's a period when they inject errors into the process. Then there are just more people to communicate to." (Fred Brooks, quoted in *Fortune*, December 12, 2005.)

Note that Brooks did not say that his law is true because we have immature processes or poor management ability. The law is true because the intellectual substance of software is profound and weighty. An architecture-centric perspective on development therefore gives some advantage in coping with problems in schedule slippage and project management; it provides a technically substantive basis for reasoning about the nascent product that is at a higher level of abstraction than source code, and provides a vehicle for conveying to new project members the principal design decisions that characterize the system.

## 2.8 End Matter

This chapter has shown how a proper view of software architecture affects every aspect of the classical software engineering activities and reorients those activities. Any practitioner can have his work informed and changed by an understanding of software architecture, to his project's benefit.

In summary,

- The requirements activity is seen as a co-equal partner with design activities, wherein previous products and designs provide the vocabulary for articulating new requirements, and wherein new design insights provide the inspiration for detailed product strategies and requirements.
- The design activity is enriched by techniques which exploit knowledge gained in previous product developments. Designing infuses the whole development and evolution process, instead of being confined to a standalone activity.
- The implementation activity is centered on creating a faithful implementation of the architecture and utilizes a variety of techniques to achieve this in a cost-effective manner, ranging from generation of the source code to utilizing implementation frameworks to reuse of pre-existing code.
- Analysis and testing activities can be focused on and guided by the architecture, offering the prospect of earlier detection of errors and more efficient and effective examinations of the product. Higher quality at a lower price should be the result.
- Evolution activities revolve around the conceptual bedrock of the product's architecture. Critically, it provides the means for reasoning about possible change and for conveying essential understandings of the product engineers new to the project.

- An equal focus on process and product results from a proper understanding of the role of software architecture in the development activity. The Turbine Model enables insight into a development process's full character, as it can reveal the extent to which activities are intermingled (likely a very good thing) and especially the extent to which the corpus of project artifacts changes over time.

Yet attempting to appropriate and apply these ideas without further detail and technical support is difficult and subject to the limitations of a designer's organization and self-discipline. It is the purpose of the following chapters to provide the representational basis for describing architectures effectively and the technological basis for incorporating architecture into a professional approach to the development of software applications.

### The Business Case for Architecture-centric Development

Sales of a product provides revenue for a company. For a company to grow, normally sales must expand through offering a range of products. For a company to retain its customer base it must be responsive to their requests for altered versions of current products as well as new offerings.

While these observations are almost trivial, the question arises as to what enables a company to perform these tasks successfully over an extended period. Again, the almost trivial answer is a sustained focus on the company's processes as well as a focus on the company's products.

What is remarkable is that over the past twenty years or so this dual focus seems to have been lost in a large number of software organizations. For many the focus has been solely a focus on process and its improvement. The results of this myopia have been rather mixed. Clearly there have been many examples of companies improving their processes and also being successful in producing high-quality, successful products. But there are also companies – much less publicized – which have achieved high-levels of process improvement but which fail to produce successful, market-leading products. The correlation between process improvement and product success is not absolute, to say the least.

In contrast, consider the relationship between a product's architecture and its quality. It is difficult to have a bad architecture and great product, a product that remains a leader after successive versions and releases. Similarly it is difficult to have a great architecture and a bad product. Unless the implementation activity is deeply flawed, a great architecture – one that emerges from design that considers all stakeholder concerns and which exhibits intellectual clarity and vision – typically will result in great products.

The correlation between a great architecture and a successful product family is perhaps even stronger. A cost-effective strategy for delivering a good product family demands intellectual coherence across the members of the product family, and cost-savings resulting from commonalities and shared infrastructure across the line.

An architecture-centric approach to software development thus puts primacy on the products that are sold and which provide a company's revenue. If process is allowed to become the primary focus, then the focus is on something that does not intrinsically generate revenue for the company. A good process is an asset – a critical one at that – but architecture, at the heart of great products, must be of primary attention.

## 2.9 Review Questions

1. Does object-oriented design impose an architecture on an application? Why or why not?
2. Is an architecture-centric viewpoint more consistent with the waterfall model or Boehm's spiral model of software development [21]? Why?
3. Suppose a feature-addition request is given to a development team that has not previously worked on the product in question. How might the team proceed if they are not in possession of the product's architecture? If they are in possession of an accurate, rich architecture?

## 2.10 Exercises

1. For some application which you have developed, describe its architecture, as built. Is that the same as the design you originally developed for the application? What accounts for any differences you observed?
2. Describe an application for which you can develop a complete, adequate requirements document without any recourse to thinking about how the system might be built. Describe an application for which you think it would be difficult, if not impossible, to describe the requirements for without recourse to architectural ("how to") concerns.
3. Investigate the history of an influential software product, such as spreadsheets (e.g. VisiCalc, Lotus 1-2-3, or Excel), or a service product (e.g. eBay or Google). What role did requirements analysis play in the development of the product? How early were design prototypes created?

4. Develop three alternative architectures for a sample problem (such as a simple video game like Tetris or an address book). What makes them different and how did you arrive at the architectures?
5. Consider the application domain of video games, in particular very simple games based around the idea of landing a spacecraft on the moon by controlling the amount of descent thrust. Create a glossary for use in requirements descriptions, including such key terms as descent rate, controls, display, and score. Do notions of solution structure affect development of the definitions? If so, how?
6. Do Exercise 5, but for the domain of spreadsheets. Make sure your glossary includes all the terms needed to fully characterize the spreadsheet's concepts
7. How does a company build market niche? How could that affect the company's approach to software processes?
8. Is it easier to build a parser for a programming language by manually programming in an object-oriented language like Java, or use a parser generator like ANTLR or Bison? What assumptions does your analysis make?
9. With regard to Exercise 8, what does implementing a parser using a parser generator entail? Where did the architecture of the (generated) parser come from?
10. With regard to Exercises 8 and 9, if you were responsible for testing both a manually written parser and a parser generated by a parser tool, how would your testing concerns and strategies vary between the two products? Why?
11. Abstract requirements may work on small problems wherein the engineer can, after specification, devise many solutions quickly, or there may only be a small number of solutions, *and* the total time involved in finding one solution starting from scratch is not so great as to matter. But above a certain threshold, it appears that it becomes either economically inefficient to pursue this course of action or it is intellectually too difficult to pursue this practice, or both. Describe a small domain where you illustrate this point. In what domains do you think that the use of abstract requirements have been most effective? To what do you attribute the success?
12. Draw a turbine model of a notional Twin Peaks software development process.
13. Draw a turbine model of a notional software project that follows the Unified Process (see [158, 161, 250] for example explications).

## 2.11 Further Reading

Substantive presentations of software engineering and software development processes may be found in any of several excellent textbooks, such as those by Ghezzi, et.al. [96], and van Vliet [299].

Problem solving and design in general has been addressed by many authors. Design is the focus of Chapter 4, and a variety of readings are listed at the end of that chapter. Polya's original book on problem solving – which largely focuses on the solving of problems in mathematics – is readily available [231]. Some general reflections on design and the design process include Schön's classic "The Reflective Practitioner" [253], Don Norman's insightful book on "The Design of Everyday Things" [205], and Nelson's treatment of the traditions and practices of design [200]. For the engineer in all of us, Henry Petroski's books exploring the design of things from bridges to paperclips are a delight, but they are especially valuable in revealing the role of failure in achieving new designs [223–226]. Several detailed stories of how design of the F-15, F-16, and A-10 aircraft were, or nearly were, subverted due to loss of focus on the core architecture are told in "Boyd: the Fighter Pilot Who Changed the Art of War" [47]. The history of the design of washing machines, mentioned briefly in the text, is presented online in a variety of websites, including <http://www.sciencetech.technomuses.ca/english/collection/wash1.cfm> and <http://www.historychannel.com/exhibits/hometech/wash.html>

Excellent presentation of contemporary thinking on the process of requirements analysis can be found in the works of Jackson, van Lamsweerde, and Nuseibeh others [138, 140, 206, 297]. Object-oriented design is explained in most modern software engineering textbooks, such as those listed above. Software analysis and testing is explained in detail in Pezze and Young's textbook [227].

The Twin Peaks model of development was presented in a short paper in IEEE Computer [207]. Subsequent work has explored more deeply the relationship between requirements and architecture; see for example [235].

## CHAPTER 3

### 3 Basic Concepts

In the preceding chapters the reader has been exposed to a number of software architectural notions, such as software components and connectors; their configurations in a given system; relationships between a system's requirements, its architecture, and its implementation; and software product lines. However, these ideas have been introduced rather informally. They have served to provide context for the field of software architecture, situate it within other facets of software engineering, and motivate its unique role and importance. Indeed, we have generally avoided definitions of terms in the hope that the reader will more readily recognize many of the discussed concepts within his own experience, or be able to relate the architectural concepts to those with which he is already familiar.

While informal terms have a useful role in introducing concepts, the uncertainties that result can hinder deeper understanding. Hence the objective of this chapter is to define the key terms and ideas from the field of software architecture, providing a uniform basis for their discussion in the remainder of the book. The reader will be exposed to the key elements of architecture-centric design and their inter-relationships, some basic techniques and processes for developing a software system's architecture, and the relevant stakeholders and their roles in architecture-based software development. We will illustrate the discussion throughout with simple examples.

#### Outline of Chapter 3

- 3 Basic Concepts
  - 3.1 Terminology
    - 3.1.1 Architecture
    - 3.1.2 Component
    - 3.1.3 Connector
    - 3.1.4 Configuration
    - 3.1.5 Architectural Style
    - 3.1.6 Architectural Pattern
  - 3.2 Models
  - 3.3 Processes

- 3.4 Stakeholders
- 3.5 End Matter
- 3.6 Review Questions
- 3.7 Exercises
- 3.8 Further Reading

## 3.1 Terminology

We begin presentation of the field's key terms with an exploration of software architecture itself and several concepts tied to it, such as architectural degradation. The major constituent elements of architectures are then explored, including components, connectors, and configurations. Two important types of potentially deep architectural knowledge are then defined and examined: architectural patterns and styles.

### 3.1.1 Architecture

At its essence, software architecture is defined quite simply, as follows.

**Definition.** A software system's *architecture* is the set of principal design decisions made about the system.

Put another way, software architecture is the blueprint for a software system's construction and evolution.

The notion of *design decision* is central to software architecture and to all the concepts based on it. For example, the special notion of *product family architectures* was briefly introduced Chapter 1. Product family architectures are anchored on the idea of reference architecture, defined as follows.

**Definition.** A *reference architecture* is the set of principal design decisions that are simultaneously applicable to multiple related systems, typically within an application domain, with explicitly defined points of variation.

Design decisions encompass every aspect of the system under development, including

- design decisions related to system *structure* – for example, “the architectural elements should be organized and composed exactly like this”;
- design decisions related to *functional behavior* – for example, “data processing, storage, and visualization will be performed in strict sequence”;

- design decisions related to *interaction* – for example, “communication among all system elements will occur only using event notifications”;
- design decisions related to the system's *non-functional properties* – for example, “the system's dependability will be ensured by replicated processing modules”, and
- design decisions related to the system's implementation – for example, the user interface components will be built using the Java Swing toolkit.

Note that in the preceding discussion and examples we have used terms such as “element” and “module”, which we have not yet defined. You can think of them simply as building blocks (akin to “bricks”) from which the architecture is composed. We will shortly address them more rigorously.

Another important term that appears in the above definitions is “principal”. It implies a degree of importance and topicality that grants a design decision “architectural status”. It also implies that not all design decisions are architectural, that is, they do not necessarily impact a system's architecture. How one defines “principal” will depend on what the system goals are. Ultimately, the system's stakeholders (including, but not restricted only to the architect) will decide which design decisions are important enough to include in the architecture, and which are not.

Based on this, note that architecture is at least in part determined by context, that non-technical considerations may end up driving it, and that different sets of stakeholders may deem different sets of design decisions principal (that is, architectural). We will discuss this further below and elsewhere in the text.

Another observation following from the definition of software architecture is that every set of “principal” design decisions can be thought of as a different architecture. Over the lifetime of a system, these design decisions will be made and unmade; they will change, evolve, “fork”, converge, and so on. As the architecture of a large, complex, long-lived system is developed and evolved, the corresponding set of architectural design decisions will be changed hundreds of times. The outcome will, in effect, be hundreds of different (though related) architectures, rather than a single architecture. In that sense, architecture has a temporal aspect.

### Prescriptive Architecture versus Descriptive Architecture

At any time,  $t$ , during the process of engineering a software system, that system's architects will have made a set of architectural design decisions,  $P$ , that reflect their intent. These design decisions comprise the system's *prescriptive architecture*. In other words, these design decisions represent

the “prescription” for the system’s construction. The prescriptive architecture is thus the system’s “as-intended” or “as-conceived” architecture. The prescriptive architecture need not necessarily exist in any tangible form. For example, it may be entirely “in the architects’ heads”. Alternatively, the prescriptive architecture may have been captured in a notation such as an architecture description language (such as those presented in Chapter 6).

Also at any point during this process, the architectural design decisions that are part of the prescriptive architecture (that is, of the set  $P$ ) will putatively be *realized* with a set of artifacts,  $A$ . These artifacts may include refinements of architectural design decisions in a notation such as the Unified Modeling Language or their implementations in a programming language. The artifacts may also include models of architectural styles and patterns used in the architecture, previously existing “off-the-shelf” software components that will be used in the desired system, implementation frameworks and middleware infrastructures that will aid the system’s construction, specifications of standards to which the architecture needs to adhere, and so on.

While many of the artifacts in  $A$  may have existed prior to and independently of the architecture under consideration, each of them embodies certain design decisions that the architects find desirable and relevant to the current system. The full set of principal design decisions,  $D$ , embodied in the set of artifacts,  $A$ , is referred to as the system’s *descriptive architecture*. The descriptive architecture is referred to as such because it “describes” how the system has been realized. The descriptive architecture is thus the system’s “as-realized” architecture.

The reader should note that, in the early stages of a system’s lifecycle, the number of artifacts that realize the architecture will typically be smaller than during later stages when more of the system’s architecture has been elaborated and possibly implemented. In fact, if we consider time  $t_1$  to indicate the inception of the initial set  $P_1$  of architectural design decisions for a given system, the sets  $A_1$ , and thus  $D_1$ , may be empty. This will typically be the case in so-called “green field” development, where the system is designed and implemented from scratch. In the case of “brown field” development, many artifacts partially realizing the architecture for a given system may exist before the architecture is even conceived; in other words, at the start of a project,  $t_0$ , the set  $D_0$  is non-empty while  $P_0$  may be an empty set. This is the case if the new system is a member of a closely related application family, the architectural styles and/or patterns that will be used are known ahead of time, the middleware platforms and/or implementation languages have been selected, and so on. Another situation in which  $P_0$  may be empty while  $D_0$  is large is development involving a legacy system whose architectural intent has been lost over

time. Such discrepancies between sets  $P$  and  $D$  can be indications of problems with a system’s software architecture, and will be discussed further below.

#### Prescriptive and Descriptive Architectures in Action – An Example

Let us illustrate the above discussion with a simple example. At this point, the reader is not expected to understand all the nuances and implications of this example, but only to follow along with the argument as it pertains to prescriptive and descriptive architecture.

Figure 3-1 shows a graphical view of the prescriptive architecture of a simple logistics application. In other words, the diagram in the figure is a model of the architecture in a graphical architecture description language. The architecture is designed using a set of components, which implement the application’s functionality, and connectors, which enable the components to call each other’s operations and exchange data. (Components and connectors will be defined more formally later in this chapter.)

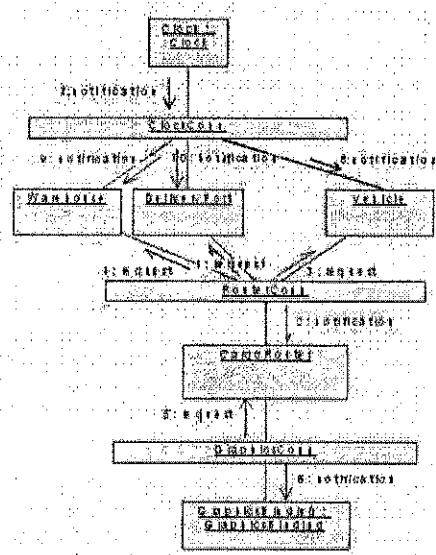
This application controls the routing of cargo from a set of incoming *Delivery Ports* to a set of *Warehouses* via a set of *Vehicles*. The *Cargo Router* component tries to optimize the use of vehicles and deliver the cargo to its proper destination (that is, warehouse). The *Clock* component provides the time and helps the ports, vehicles, and warehouses to synchronize as necessary. Finally, the *Graphics Binding* component provides a graphical user interface that allows a human operator to assess the state of the system during its execution. The components in the system interact via three connectors—*Clock Conn*, *Router Conn*, and *Graphics Conn*—by exchanging requests and replies. The lines connecting the component and connector elements in the architecture represent the elements’ interaction paths.

**Figure 3-1.** A high-level graphical view of the prescriptive (that is, “as-designed” or “as-intended”) architecture of the cargo routing application.

This is a UML activity diagram drawn in IBM/Rational Rose [236]. Only a subset of the interactions among the components and connectors are depicted.

The cargo routing application is useful in this discussion for three reasons. First, its simplicity suggests that its architects should have been able to evaluate all of the architectural decisions and their trade-offs before the application was implemented. Second, the architecture was carefully implemented with the help of an architectural framework (see Chapter 6 for a discussion of architectural frameworks), which allowed the application’s developers to realize all of the architectural design decisions directly in the code. Third, aside from a GUI library, no other off-the-shelf functionality was used in the implementation, which allowed for a carefully controlled mapping between the architecture and its implementation (that is, between the sets  $P$  and  $D$ ).

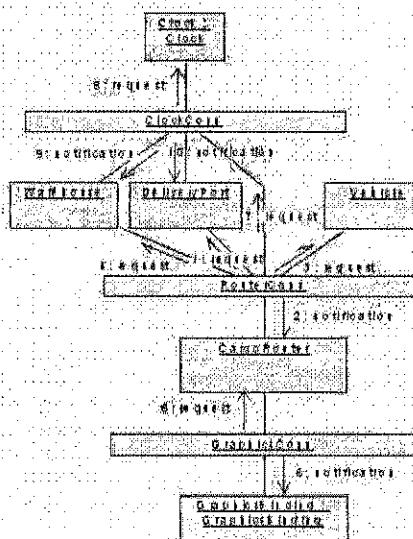
A graphical view of the descriptive (that is, as-realized) architecture of the cargo routing application is depicted in Figure 3-2. While there are many artifacts in the set  $A$  of this application (including the architectural style used to realize the architecture, the implementation framework, the off-the-shelf GUI toolkit, and the implementation code itself), we have deliberately elided many of these and extracted the simplified view of the descriptive architecture,  $D$ , from them.



**Figure 3-2.** A high-level, graphical view of the descriptive (that is, “as-implemented” or “as-realized”) architecture of the cargo routing application.

This is a UML activity diagram drawn in IBM/Rational Rose. Only a subset of the interactions among the components and connectors are depicted.

It can be noticed immediately that the extracted view of the descriptive architecture is not identical to the prescriptive architecture: the *Vehicle* component is not connected to the *Clock Conn* connector, while the *Router Conn* and *Clock Conn* connectors are connected, allowing “two hop” routing of requests and replies in the architecture. It is thus possible for the *Clock* component to interact directly with the *Cargo Router* component via the two connectors. The application-specific reasons behind these changes are unimportant to this discussion. What is important is the fact that the programmers and architects together discovered that, even in the case of such a simple application, they had not properly thought through all of the architectural design decisions. It is, then, reasonable to expect that such issues would only be exacerbated in larger, more complex systems.



Let us take this discussion a step further. We can ask several questions about the prescriptive and descriptive architectures of the cargo routing application. Again, the reader is not yet expected to be able to provide complete answers to these questions. Instead, the purpose is to illustrate certain issues that will be revisited throughout the remainder of this book, and sensitize the reader to the difficulties inherent in the architectural design of even moderately complex software systems.

1. Which architecture is “correct”? The prescriptive architecture reflects the architects’ intent; but the descriptive architecture reflects the added experience of actually implementing the system.
2. Are the two architectures consistent with one another? In this example the differences were relatively easy to spot. However, architectural inconsistencies can be much more complex and/or insidious.
3. What criteria are used to establish the consistency between the two architectures? Again, in this example a simple structural comparison sufficed, but more sophisticated techniques may be needed.
4. On what information is the answer to the preceding questions based? The two diagrams in Figure 3-1 and Figure 3-2 represent very small subsets of different concerns that may be captured and/or visualized in an architectural model. Even if these two diagrams were identical, the amount of architectural information they represent is insufficient to make any guarantees about the two architectures’ relationship.

We will further elaborate on the issue of architectural consistency next.

### Architectural Degradation

During the lifespan of a typical software system, a large number of prescriptive and descriptive architectures will be created. Each corresponding pair of such architectures represents the system’s software architecture at a given time,  $t$ . As the set of principal design decisions,  $P$ , the set of artifacts,  $A$ , and the corresponding principal design decisions,  $D$ , embodied in the artifacts, grow, so the system’s software architecture becomes more complete. The system’s stakeholders will decide the state at which  $P$  and  $A$  (and thus  $D$ ) can be considered sufficiently complete and sufficiently consistent with one another for the system to be released into operation.

In an ideal scenario, the two sets of architectural design decisions,  $P$  and  $D$ , would always be identical; in other words,  $D$  would always be a perfect realization of  $P$ . However, this need not be the case. For example, an off-the-shelf component or middleware platform will likely embody a number of design decisions which may, in turn, impact the architectural design decisions made for the system under construction. Thus, the exact relationship between sets  $P$  and  $D$  may vary depending on the system in question, the requirements imposed by system stakeholders, the point in the system’s lifespan, and so on. However, it is imperative that the

stakeholders, and architects in particular, understand this relationship and be precise about the allowed differences between  $P$  and  $D$ .

Note that, given sets of design decisions in  $P$  and  $D$  at time  $t$ , it is possible for these sets to remain stable to time  $t+n$ . This simply means that though the set  $A$  may have enlarged as implementation progresses, the addition of more artifacts or the further development of existing artifacts did not introduce any new principal decisions. It is also possible that  $P$  changes while  $D$  remains the same (e.g., when architectural design concerns are elaborated but the artifacts realizing the system have not yet been updated); similarly  $D$  may change while  $P$  remains the same.

When a system is initially developed or when the already implemented system is evolved, ideally its prescriptive architecture is first modified appropriately, and then the corresponding changes to the descriptive architecture follow. Unfortunately, this does not always happen in practice. Instead the system (and thus its descriptive architecture) is often directly modified, without accounting for the impact relative to the prescriptive architecture.

In the above example of the cargo routing application, the developers may not have bothered to inform the architects that they decided to change the architecture in several places – even if those changes were warranted. This failure to update the prescriptive architecture happens for several reasons: developer sloppiness, perception of short deadlines which prevent thinking through and documenting the impact on the prescriptive architecture, lack of a documented prescriptive architecture, need or desire to optimize the system “which can only be done in the code”, inadequate techniques and tool support, and so forth.

Whatever the reasons, they are flawed and potentially dangerous, especially if one considers that software systems are notorious for containing many errors (that is, for being “buggy”): do we really want the as-realized architecture, with all of its potentially latent faults, to be the final arbiter of the architects’ intent? The resulting discrepancy between a system’s prescriptive and descriptive architecture is referred to as *architectural degradation*. Architectural degradation comprises two related phenomena: *architectural drift* and *architectural erosion*.

**Definition.** *Architectural drift* is introduction of principal design decisions into a system’s descriptive architecture that (a) are not included in, encompassed by, or implied by the prescriptive architecture, but which (b) do not violate any of the prescriptive architecture’s design decisions.

Architectural drift does not necessarily result in outright violations of the prescriptive architecture. Instead, it circumvents the prescriptive architecture, and may involve decisions whose implications are not properly understood and which may affect the given system's future adaptability.

Drift is a result of direct changes to the set,  $A$ , of system artifacts. These changes may, in turn, result in changes to the set,  $D$ , of corresponding principal design decisions. Note that all expansions of the set  $D$  do not necessarily result in architectural drift. New, principal decisions may be added to  $D$  (as the result of adding or changing elements of  $A$ ) that are consistent with all the decisions in  $P$  and that are implied by or encompassed by decisions in  $P$ . For instance,  $P$  may require encryption to be used in any communication over an open network;  $D$  may state that public-key algorithms be used to support such encrypted communication – a decision encompassed by  $P$ .

As an example of architectural drift, the descriptive architecture in the cargo routing application (Figure 3-2) reflects the architectural design decision to introduce a link between two connectors, which did not exist in the prescriptive architecture. Assuming that the system's original architects did not explicitly prohibit the direct linking of two connectors, adding the link would not violate any of the architectural decisions made in the prescriptive architecture. However, it does not mean that adding this link was a harmless or proper thing to do.

Architectural drift may also cause violations of architectural style rules. In other words, architectural drift reflects the engineers' insensitivity to the system's architecture and can lead to a loss of clarity of form and system understanding [221]. If not properly addressed, architectural drift will eventually result in architectural erosion.

**Definition.** *Architectural erosion* is the introduction of architectural design decisions into a system's descriptive architecture that violate its prescriptive architecture.

In terms of the architectural design decision sets,  $P$  and  $D$ , architectural erosion can be thought of as the result of direct changes to the system artifact set,  $A$ , which introduces a principal design decision in  $D$  that invalidates or violates one or more design decisions that already exist in  $P$ . Erosion renders a system difficult to understand and adapt, and also frequently leads to system failure.

Architectural erosion can easily occur when a system has “drifted too far,” in that it is easy to violate important architectural decisions if those decisions are obscured by many small, intermediate changes. Note that an

architecture can certainly erode without previous drift. However, this is both less likely to happen (since there has been no drift yet, the prescriptive and descriptive architectures are consistent at the time the erroneous changes are made), and easier to recover from, since fewer decisions are involved. Note also that architectural erosion may be caused by design decisions that are sound when considered in isolation. However, in combination with other decisions that have been made, but perhaps not properly documented, a new design decision may have unforeseen and undesired consequences.

In the cargo routing application example, the removal of the link between the *Vehicle* component and its adjacent connector in the descriptive architecture would have resulted in architectural erosion had it not been justified and had the prescriptive architecture not been properly updated. The removal of this link introduces the potential danger that the vehicles controlled by the system are unable to synchronize properly with the rest of the system and deliver their cargo on time. In this case, the system developers realized that vehicles do not need to keep track of time internally so long as the *Cargo Router* component gives them appropriate instructions. They discussed this observation with the architects, who agreed and updated the prescriptive architecture accordingly.

Both architectural drift and architectural erosion can be dangerous and expensive, and should be avoided. This requires a certain discipline on the part of architects and developers, but in the long run it will save effort and money, while helping to preserve the important system properties.

### Architectural Perspectives

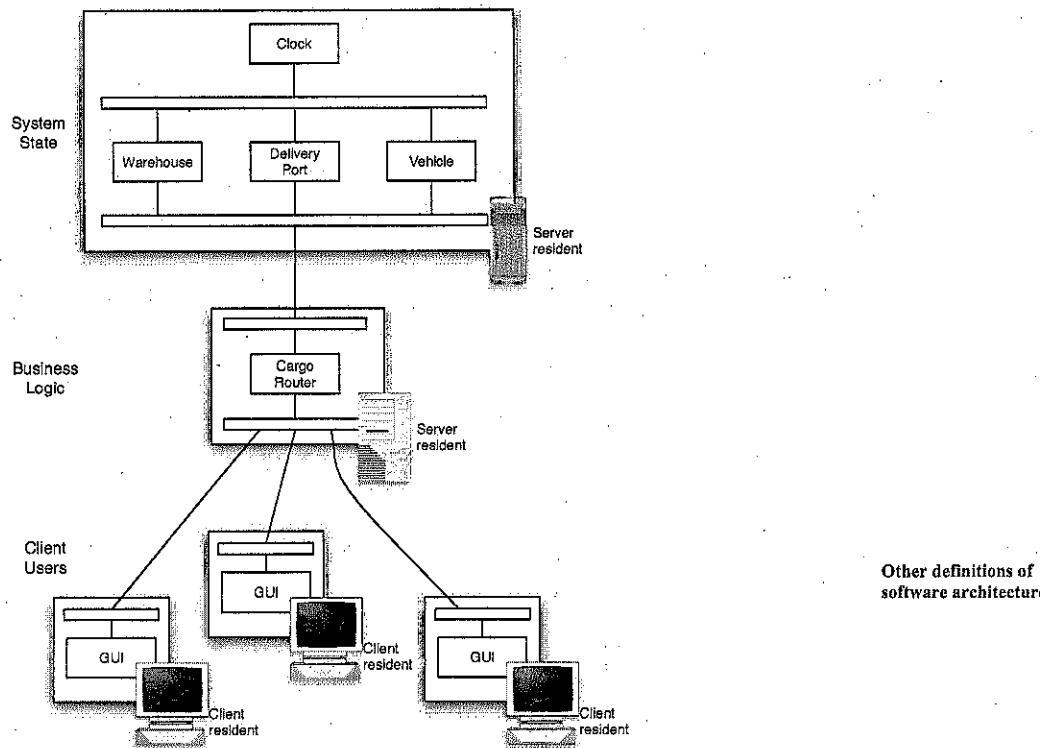
The notion of an architectural perspective is to highlight some aspects of an architecture while eliding others.

**Definition.** An *architectural perspective* is a non-empty set of types of architectural design decisions.

As the preceding discussion has indicated, software architectures encompass decisions made by a variety of stakeholders at varying levels of detail and abstraction. The purpose of an architectural perspective is to direct attention, for example for purposes of analysis, to a subset of the decisions.

An example perspective is *deployment*. A software system cannot fulfill its purpose until it is deployed, that is, until its executable modules are physically placed on the hardware devices on which they are intended to run. The deployment perspective of an architecture can be critical in assessing whether the system will be able to satisfy its requirements. For example, placing many large components on a small device with limited

memory and CPU power, or transferring high volumes of data over a network link with low bandwidth will negatively impact the system, much like incorrectly implementing its functionality will. An example deployment perspective on the cargo routing application's architecture is shown in Figure 3-3.



**Figure 3-3.** A deployment view of the cargo routing application's architecture distributed across five devices. It is assumed that the Warehouse, Delivery Port, and Vehicle components interact with the corresponding physical objects in order to be able to maintain their state in real-time. However, those interactions are not depicted here.

To further illustrate, recall that architecture has a temporal dimension, that is, that a system's architecture will likely change over time. However, at any given point in time, the system has only *one* architecture. That architecture may be thought of, modeled, visualized, and discussed from different perspectives. For example, the perspective of the system's modules and their interconnections that is unencumbered with any aspects

of the hardware on which the system will run might be referred to as the *structural view*; if we were talking about the prescriptive architecture of a system, then we would say that this is the *structural view of the prescriptive architecture*; if, on the other hand, we were to postulate the hardware topology on which this architecture may (or should) run once implemented, then we would be talking about the *deployment view of the prescriptive architecture*; if we are discussing the distribution of implemented system modules on the different hardware hosts, we would say that this is the *deployment view of the descriptive architecture*; and so on.

Architectural perspectives and views will be discussed in more detail in Chapters 6 and 7. We continue the discussion below with definitions of key architectural building blocks and several other key concepts derived from the concept of software architecture.

Perry and Wolf [221] provide a useful characterization of software architecture as a triple:

**Definition.** Architecture = {elements, form, rationale}

In other words, the architecture defines the system's key elements, and their relationships to each other and to their environment. Furthermore, the architecture reflects the rationale behind the system's structure, functionality, interactions, and resulting properties.

Elements capture the system's building blocks, and help to answer the "what" questions about the architecture. The questions you may ask about the architecture's elements include the following: What are the system's building blocks? What is a given element's primary purpose in the system? What system services does each element (help to) provide?

Perry and Wolf identify three types of building blocks:

- processing elements,
- data elements, and
- connecting elements.

These three types are usually consolidated into two major architectural concepts, components and connectors, which will be discussed below. The one notable exception is the REST architectural style, which was introduced in Chapter 1 and will be further discussed in Chapter 11: REST not only gives data elements first-class status, they surpass in importance both processing and connecting elements.

The form captures the way in which the system elements are organized in the architecture. Form represents the structure of individual architectural

elements, the manner in which they are composed in the system (that is, the architecture's configuration or topology), the characteristics of their interaction, as well as their relationship to their operating environment (e.g., deployment of specific software elements onto specific hardware hosts). The form helps to answer the "how" questions about the architecture, which may include the following: How is the overall architecture organized? How are the elements composed to accomplish the system's key tasks? How are the elements distributed over a network?

Finally, rationale represents the system designers' intent, assumptions, subtle choices, external (perhaps non-technical) constraints, selected design patterns and styles, and any other information that may not be obvious or easily derivable from the architecture. Rationale helps to answer the "why" questions about the architecture. These questions may include the following: Why are particular elements used? Why are they combined in a particular way? Why is the system distributed in the given manner?

Although in their seminal paper Perry and Wolf acknowledge the key role of software architecture in a system's evolution, note that their definition does not explicitly capture evolution. However, their definition does suggest that capturing the design rationale is a prerequisite to successfully making any subsequent changes to the system's architecture.

Another useful definition of architecture, which explicitly addresses system evolution, is that provided by the *ANSI/IEEE Standard 1471-2000, Recommended Practice for Architectural Description of Software-Intensive Systems*.

**Definition.** Architecture is the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution.

Note that this definition does not specifically refer to software, suggesting that the architecture of a software system is fundamentally similar to architectures of other types of complex systems.

Another interesting, and frequently cited definition of software architecture is attributed to Chris Verhoef [153].

**Definition.** The software architecture of deployed software is determined by those aspects that are the hardest to change.

This is a different perspective on how to define software architecture: the

definition tells us what *effect* architecture will have on a software system in terms of that system's stability and modifiability. However, the definition does not say what architecture *is*. Furthermore, it is a fair question to ask whether just because something is principal it must be "hardest" to change? In fact, in many cases, architectural design decisions will be explicit enablers of system modification. Examples of this will be provided throughout the book, and in particular in the discussion of architecture-driven software system adaptation discussed in Chapter 14.

### 3.1.2 Component

The decisions comprising a software system's architecture encompass a rich interplay and composition of many different elements. These elements address key system concerns, including:

- processing, which may also be referred to as functionality or behavior,
- state, which may also be referred to as information or data, and
- interaction, which may also be referred to as interconnection, communication, coordination, or mediation.

In this section we will address architectural elements dealing with the first two concerns—processing and data. In the next section we will address interaction.

Elements that encapsulate processing and data in a system's architecture are referred to as *software components*.

**Definition.** A *software component* is an architectural entity that (1) encapsulates a subset of the system's functionality and/or data, (2) restricts access to that subset via an explicitly defined interface, and (3) has explicitly defined dependencies on its required execution context.

Put another way, a software component is a locus of computation and state in a system [257]. A component can be as simple as a single operation or as complex as an entire system, depending on the architecture, the perspective taken by the designers, and the needs of the given system. The key aspect of any component is that it can be "seen" by its users, whether human or software, from the "outside" only, and only via the interface it (or, rather, its developer) has chosen to make public. Otherwise it appears as a "black box". Software components are thus embodiments of the software engineering principles of *encapsulation*, *abstraction*, and *modularity*. In turn, this has a number of positive implications on a component's composability, reusability, and evolvability.

Another critical facet of software components that makes them usable and reusable across applications is their explicit treatment of the execution context that a component assumes and on which it depends. The extent of the context captured by a component can include

- the component's *required* interface, that is, the interface to services provided other components in a system on which this component depends for its ability to perform its operations;
- the availability of specific resources, such as data files or directories, on which the component relies;
- the required system software, such as programming language runtimes, middleware platforms, operating systems, network protocols, device drivers, and so on;
- the hardware configurations needed to execute the component;
- and so on.

Another aspect of a software component, and one that helps to distinguish it further from the connectors discussed below, is a component's relationship to the specific application to which it belongs. Components are often targeted at the processing and data capture needs of a particular application, that is, they are said to be *application-specific*. For example, *Vehicle* and *Warehouse* in the cargo routing system are application-specific components: while they may be useful in other similar systems, they were specifically designed and implemented to address the needs of this application.

This need not be always the case however. Sometimes components are designed to address the needs of multiple applications within a particular class of applications or problem domain. For example, Web servers are an integral part of any Web-based system; one will probably download, install and configure an existing Web server rather than develop one's own. Another example are components such as *CTunerDriver*, *CFrontEnd*, and *CBackEnd*, introduced in product-line discussion in Chapter 1, which are intended to be reused across different systems within the consumer electronics domain.

Finally, certain software components are "utilities" that are needed and can be reused across numerous applications, without regard for the specific application characteristics or domain. Common examples of reusable utility components are math libraries and GUI toolkits, such as Java's Swing toolkit. Another example of arbitrarily reusable components is that of common off-the-shelf applications such as word processors, spreadsheets, or drawing packages. While they usually provide a large superset of any one system's particular needs, architects may choose to integrate them rather than reimplement the exact needed functionality. As the reader will recall, this is the very reason why a system's prescriptive and descriptive architecture need not be identical.

Szyperski provides another, widely cited definition of software component [271]. He approaches components from a somewhat different perspective.

**Definition:** A software component is a unit of composition with contractually specified interfaces and explicit context dependencies only. A software component can be deployed independently and is subject to composition by third parties.

This definition does not tell us what a component is, but rather how it is to be structured and used, both by software developers (by composing the component into a system and deploying it) and by other components (by interacting with it through explicit interfaces). This definition also reflects the vision that, once engineered, the component's interior becomes invisible to the outside world. At the same time, the definition does not capture the role a component plays in a system, so that the same definition could in fact be used to define a software connector. Below we will define what a software connector is, and how it fundamentally differs from a component.

#### Other definitions of software component

Szyperski's definition is similar to several other definitions of software components in that it does not separate processing from data components as suggested by Perry and Wolf. It is possible that this failure to separate data from computation in software systems' architectures is a side effect of the popularity of object-orientation and particularly object-oriented languages, in which all system elements are treated as objects regardless of their purpose. One of the primary goals of software architectures is to illuminate and improve understanding of software systems, however, and it may be argued that different concerns (in this case, processing components and data components) should be treated separately. Even though our definition does identify the dual purpose of software components, we should point out that we have rarely found the two addressed separately (the REST architectural style being one notable example); instead, most frequently a single component will perform a portion of the system's functionality and maintain a part of its state. The distinction will, then, be made according to the component's primary purpose in the system.

### 3.1.3 Connector

Components are in charge of *processing* and *data*. Another fundamental aspect of software systems is *interaction* among the system's building blocks. Many modern systems are built from large numbers of complex components, distributed across multiple, possibly mobile hosts, and dynamically updated over long time periods. In such systems, ensuring

appropriate interactions among the components may become even more important and challenging to developers than the functionality of the individual components. In other words, the interactions in a system become a principal (that is, architectural) concern. Software connectors are the architectural abstraction tasked with managing component interactions.

**Definition.** A software connector is an architectural element tasked with effecting and regulating interactions among components.

In traditional desktop software systems, connectors have usually manifested themselves as simple procedure calls or shared data accesses, and have typically been treated as ephemeral or invisible in terms of architecture. This is emblematic of “boxes and lines” diagrams, where the boxes, that is, components, dominate, while connectors are relegated to a minor role and accordingly represented as lines without identity or any unique or important properties. Furthermore, these simple connectors are usually restricted to enabling the interaction of pairs of components. However, as software systems have become more complex, so have connectors, with their own separate identities, roles, and bodies of implementation-level code, as well as ability to simultaneously service many different components.

Connectors are such a critical, rich, and yet largely underappreciated element of software architectures that we have decided to dedicate an entire chapter to them (Chapter 5). Here we will just briefly illustrate some of the connectors with which the reader may be familiar.

The simplest and most widely used type of connector is *procedure call*. Procedure calls are directly implemented in programming languages, where they typically enable synchronous exchange of data and control between pairs of components: the invoking component (the “caller”) passes the thread of control, as well as data in the form of invocation parameters, to the invoked component (the “callee”); after it completes the requested operation, the callee returns the control, as well as any results of the operation, to the caller.

Another very common connector type is *shared data access*. This connector type is manifested in software systems in the form of non-local variables or shared memory. Connectors of this type allow multiple software components to interact by reading from and writing to the shared facilities. The interaction is distributed in time, that is, asynchronous: the writers need not have any temporal dependencies or place any temporal constraints on the readers, and vice versa.

An important class of connectors in modern software systems is *distribution* connectors. These connectors typically encapsulate network library APIs to enable components in a distributed system to interact. A distribution connector is usually coupled with a more basic connector to insulate the interacting components from the system distribution details. Thus, for example, remote procedure call (RPC) connectors couple distribution support with procedure calls.

Many software systems are constructed from pre-existing components, which may not have been tailor-made for the given system. In such cases, the component may need “help” with integrating and interacting with one another. *Adaptor* connectors are employed to this end. Depending on their characteristics and the context within which they are used, at least two common kinds of adaptor connectors with which the reader may be familiar are wrappers and glue code.

Note that while components mostly provide application-specific services, connectors are typically application-independent. We can discuss the characteristics of a procedure call, distributor, adaptor, and so forth independently of the components they service. Notions that have entered our collective dialect, such as “publish-subscribe”, “asynchronous event notification”, “remote procedure call”, and so forth, have associated meanings and characteristics that are largely independent of the context within which they are used. Such connectors can be built without a specific purpose in mind, and then used in applications repeatedly (possibly after some customization).

### 3.1.4 Configuration

Components and connectors are composed in a specific way in a given system’s architecture to accomplish that system’s objective. That composition represents the system’s configuration, also referred to as topology. We define configurations as follows.

**Definition.** An *architectural configuration* is a set of specific associations between the components and connectors of a software system’s architecture.

A configuration may be represented as a graph wherein nodes represent components and connectors, and whose edges represent their associations (topology or “interconnectivity”).

As an example, Figure 3-1 shows the architectural configuration of the example cargo routing system. In the figure, *Delivery Port* and *Cargo Router* are examples of components, while *Router Conn* is a connector between them. The configuration shown in the diagram implies that it is possible for these two components to interact with one another, that is, that

there is a possible interaction *path* between the components. However, the displayed information does not guarantee their actual ability to interact. In addition to the appropriate connectivity, the components must have compatible interfaces; note that interfaces are not shown in the diagram in Figure 3-1. Incompatible interfaces are one source of *architectural mismatch*. We will further discuss the issue of architectural mismatch below.

### 3.1.5 Architectural Style

As software engineers have built many different systems across a multitude of application domains they have observed that, under given circumstances, certain design choices regularly result in solutions with superior properties. Compared to other possible alternatives, solutions such as this are more elegant, effective, efficient, dependable, evolvable, scalable, and so on. For example, it has been observed that the following set of design choices ensures effective provision of services to multiple system users in a distributed setting. These choices are intentionally stated here informally, to illustrate the point.

1. Physically separate the software components used to request services from the components that provide the needed services, to allow for proper distribution and scaling up, both in the numbers of service providers and service requesters.
2. Make the service providers unaware of the requesters' identity to allow the providers to service transparently many, possibly changing requesters.
3. Insulate the requesters from one another to allow for their independent addition, removal, and modification. Make the requesters dependent only on the service providers.
4. Allow for multiple service providers to "emerge" dynamically to off-load the existing providers should the demand for services increase above a given threshold.

Note that the above list does not comprise architectural design decisions for a particular system (or class of systems). Rather, these architectural decisions are applicable to any system that shares the distributed service provision context. These decisions do not specify the components (or component types), the interaction mechanisms among those components, or their specific configuration. The architect will have to elaborate further on these decisions and turn them into application-specific architectural decisions when designing a system. These higher-level architectural decisions do, however, state the rationale that underlies them, so that the architect can justify choosing them for his system.

**Definition.** An *architectural style* is a named collection of architectural design decisions that (1) are applicable in a given development context, (2) constrain architectural design decisions that are specific to a particular system within that context, and (3) elicit beneficial qualities in each resulting system.

The above example is an informal and partial specification of the popular client-server style. Many other styles are in use regularly in software systems. The REST and pipe-and-filter styles were introduced in Chapter 1. These and others will be revisited throughout the book. Those readers especially interested in architectural styles will find detailed discussions in Chapters 4 and 11.

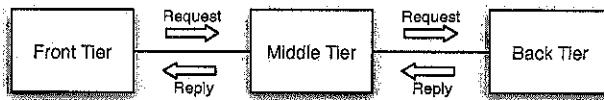
### 3.1.6 Architectural Pattern

Architectural styles provide general design decisions that both constrain and may need to be refined into additional, usually more specific design decisions in order to be applied to a system. In contrast, an architectural pattern provides a set of specific design decisions that have been identified as effective for organizing certain classes of software systems or, more typically, specific subsystems. These design decisions can be thought of as configurable in that they need to be instantiated with the components and connectors particular to an application. In other words:

**Definition.** An *architectural pattern* is a set of architectural design decisions that are applicable to a recurring design problem, and parameterized to account for different software development contexts in which that problem appears.

An example pattern that is used widely in modern distributed systems is the *three-tier system* pattern. The three-tier pattern is applicable to many types of systems in which distributed users need to process, store, and retrieve significant amounts of data: science (for example, cancer research, astronomy, geology, weather), banking, electronic commerce, reservation systems across widely different domains (for example, travel, entertainment, medical care), and so on. Figure 3-4 shows an informal graphical view of this pattern.

Figure 3-4. Graphical view of the three-tier system architectural pattern.



In this pattern, the first tier, often referred to as the “front” or “client” tier, contains the functionality needed to access the system’s services, typically by a human user. The front tier would thus contain the system’s GUI, and possibly be able to cache data and perform some minor local processing. It is assumed that the front tier is deployed on a standard host (for example, a desktop PC) possibly with limited computing and storage capacity. It is also assumed that the front tier will be replicated to allow independent, simultaneous access to multiple users.

The second tier, also referred to as the “middle”, “application”, or “business logic” tier contains the application’s major functionality. The middle tier is in charge of all significant processing, servicing requests from the front tier, and accessing and processing data from the back tier. It is assumed that the middle tier will be deployed on a set of powerful and capacious “server” hosts. However, the number of middle tier hosts is usually significantly smaller than the number of front tier hosts.

Finally, the third tier, also referred to as the “back”, “back-end”, or “data” tier contains the application’s data access and storage functionality. Typically this tier will host a powerful database that is capable of servicing many data access requests in parallel.

The interactions among the tiers in principle obey the request-reply paradigm. At the same time, the pattern does not prescribe those interactions further. For example, it may be possible to design and implement a three-tier-compliant system to strictly adhere to synchronous, request triggered, single request-single reply interaction; alternatively, it may be possible to allow multiple requests to result in a single reply, multiple replies to be issued in response to a single request, periodic updates to be issued from the back and middle tiers to the front tier, and so forth.

The three-tier architectural pattern can be used to determine the architecture of a specific distributed software system. The things the architect needs to specify are:

1. which application-specific user interface, processing, and data access and storage facilities are needed and how they should be organized within each tier, and

2. which mechanisms should be used to enable interaction across the tiers.

Use of architectural styles to solve the same problem requires, in contrast, more attention from the system’s architect, and provides less direct support. In fact, the three-tier architectural pattern can be thought of as two specific architectures that are designed according to the client-server style and overlaid on top of each other: the front tier is the client to the middle tier, while the middle tier is the client to the back tier; the middle tier is thus a server in the first client-server architecture and a client in the second. Indeed, systems adhering to the client-server style are frequently referred to two-tier systems.

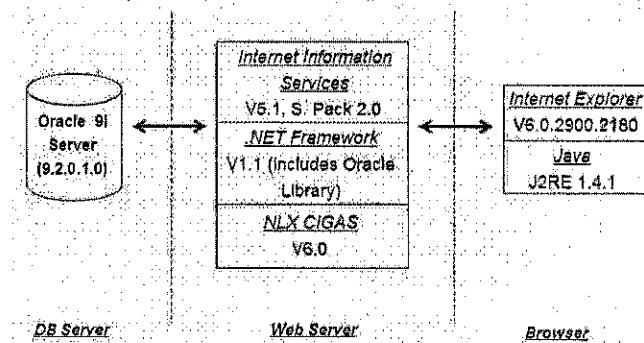
As an example, Figure 3-5 shows architectures of two different three-tier systems. At this point, the reader should be able to identify some architectural traits the two systems have in common, and those that differ.

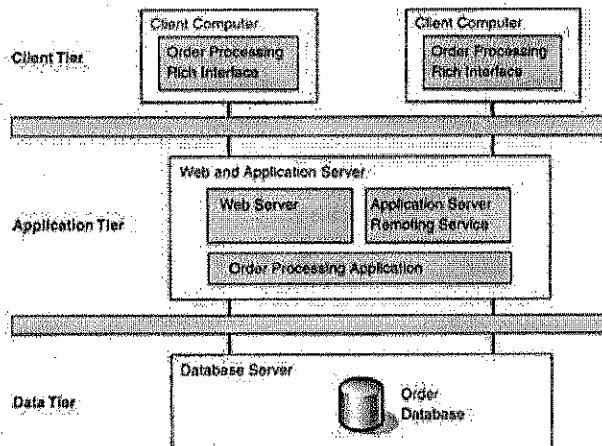
Further discussion and additional examples of architectural patterns can be found in Chapter 4. That chapter also discusses the fuzzy boundary between patterns and styles. While the definitions above distinguish the concepts, in practice the two notions can become blurred.

## Overview of System Architecture

Figure 3-5. Two example three-tier system architectures. Simply “Googling” the phrase will yield many hits.

@@Either credit these diagrams or redraw/replace





## 3.2 Models

A software system's architecture is captured in an architectural *model* using a particular modeling *notation*.

**Definitions.** An architectural *model* is an artifact that captures some or all of the design decisions that comprise a system's architecture. Architectural *modeling* is the reification and documentation of those design decisions.

A model is a result of the activity of modeling, which constitutes a significant portion of a software architect's responsibilities. One system may have many distinct models associated with it. Models may vary in the amount of detail they capture, their specific foci (e.g., structural vs. behavioral, static vs. dynamic, entire system vs. a particular component or subsystem), the type of notation they use, and so forth.

**Definition.** An architectural modeling *notation* is a language or means of capturing design decisions.

For example, the two diagrams shown in Figure 3-5 above represent models captured in two different visual modeling notations. The notations for modeling software architectures are frequently referred to as architecture description languages (ADLs). ADLs can be textual or graphical, informal (e.g., Power Point diagrams), semi-formal, or formal,

domain-specific or general-purpose, proprietary or standardized, and so on.

Architectural models are used as the foundation for most other activities in architecture-based software development processes, such as analysis, system implementation, deployment, and dynamic adaptation. Models and modeling are critical facets of software architecture and are discussed in depth in Chapter 6.

## 3.3 Processes

As discussed at length in Chapter 2, software architecture is not a software engineering lifecycle phase that follows requirements elicitation and precedes low-level design and system implementation. Instead, it permeates, is an integral element of, and is continually impacted by, all facets of software systems development. In that sense, software architecture helps to anchor the processes associated with different development activities. Each of these activities is covered separately in this book. With one exception, we will only name them here and point the reader to the chapter in which they are discussed:

- the activity of architectural *design* (Chapter 4);
- architecture *modeling* (Chapter 6) and *visualization* (Chapter 7);
- architecture-driven system *analysis* (Chapter 8);
- architecture-driven system *implementation* (Chapter 9);
- architecture-driven system *deployment*, runtime *redeployment*, and *mobility* (Chapter 10);
- architecture-based *design for non-functional properties* (Chapter 12), including security and trust (Chapter 13); and
- architectural *adaptation* (Chapter 14).

The one activity on which we will focus in this section is *architectural recovery*. Architectural recovery is again revisited in Chapter 4, in the context of architectural design processes, and in Chapter 8, in the context of architectural analysis.

Recall the above discussion of architectural degradation (that is, architectural drift and/or erosion). If degradation is allowed to occur, a software development organization is likely to be forced to *recover* the system's architecture sooner or later. This happens when, at time *t* during a system's life, changes to the system become too expensive to implement and their effects too unpredictable because the documented prescriptive (that is, *as-intended*) architecture is so outdated as to be useless or, sometimes even worse, misleading.

**Definition.** *Architectural recovery* is the process of determining a software system's architecture from its implementation artifacts.

Implementation artifacts can be source code, executable files, Java .class files, and so forth. As an illustration, Figure 3-6 shows the dependencies among the Java objects that implement the cargo routing application introduced in section 3.1.1. This diagram has been automatically generated from the application's source code using an off-the-shelf source code analysis tool. At this magnification the figure is used for illustration only; we do not expect the reader to understand its details, other than that the rectangles, which are mostly on the left, represent objects and the lines, extending to the right, represent dependencies between them (for example, Java method calls).

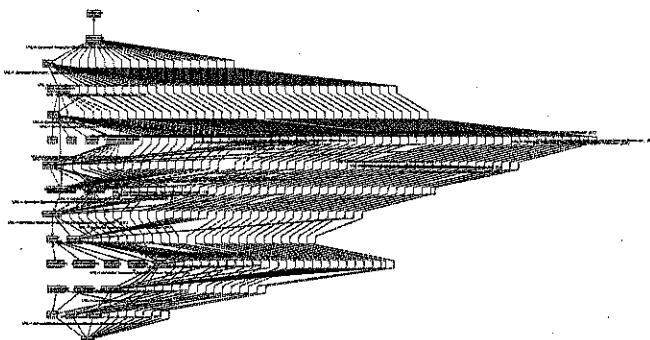


Figure 3-6.  
Implementation-level  
view of the cargo  
routing application.

Figure 3-6 reflects many details: architectural design decisions, low-level design decisions, implementation-level decisions, the Java libraries used by the system, the implementation framework, and so on. From derived artifacts such as this, the system's architecture is recovered by the process of isolating and extracting only the architectural — that is, principal — design decisions.

By its very nature, the process of architectural recovery extracts a system's *descriptive* architecture. That architecture, if complemented with statement of the architects' original intent, can in principle be used to recover the system's *prescriptive* architecture. However, since the original architects may be unavailable, and their original intent may not have been recorded (or, even if it was recorded originally, may have been repeatedly violated over time), it is often impossible to recover a system's prescriptive architecture. Instead, the recovered descriptive architecture is treated as the closest approximation of the system's prescriptive architecture, and thus the system's architectural evolution clock is "reset".

Additional details on the manner in which architectural recovery can be performed will be provided in Chapters 4 and 8. Even though the specifics of the architectural recovery tools and techniques used in practice are beyond the scope of this chapter, the reader should appreciate that recovery is a very time consuming and complex process. Furthermore, the sheer complexity of most software systems —with their myriad explicit, implicit, intended, and unintended module inter-dependencies— makes the task of assessing a given implementation's compliance to its purported architecture very difficult. This is why it is critical for software architects and engineers to maintain architectural integrity at *every* step throughout the system's lifespan. Once the architecture degrades, all subsequent solutions to stem that degradation will be more costly and more error prone by comparison.

### 3.4 Stakeholders

The preceding sections have introduced the reader to the "what", the "how", and they "why" of software architecture. This section rounds out the chapter by briefly introducing the "who", that is, several key architectural stakeholders. A much more complete treatment of architectural stakeholders will be provided in Chapter 17.

The software *architect* is one obvious stakeholder. The architect conceives the system's architecture, and then models, assesses, prototypes, and evolves it. Architects are the maintainers of a system's conceptual integrity, and are thus the system's critical stakeholders.

Software *developers* are the primary consumers of an architect's product (that is, the architecture). They will realize the principal design decisions embodied in the architecture by producing a system implementation.

The role of software *managers* from an architectural standpoint is to provide project oversight and support for the software architects. As will be detailed in Chapter 17, in an organization architects often bear much of the responsibility for a system's success without the accompanying authority. This is why it is critical for architects and managers to work closely together, and for the managers to buy into the key architectural decisions and, if necessary, exert their authority on behalf of the architects. Managers are thus key stakeholders as well.

The bottom line objective for a given system's *customers* — the ultimate stakeholders — is that a high-quality system satisfying their requirements be delivered on time and within budget. A significant determinant of a project's ability to meet that objective will be the system's architecture. Simply put, an effective architecture will result in a successful project, while an ineffective one will seriously hamper the project's success.

### 3.5 End Matter

Any mature engineering field must be accompanied by a shared, precise understanding of its basic concepts, commonly used models, and processes. This chapter has defined the notions that underlie the field of software architecture. While a less experienced reader may not yet be able to fully appreciate some of the definitions and accompanying discussion, in subsequent chapters we will repeatedly return to these concepts as we study them in greater depth. We expect that the reader will also find it useful to return to these concepts and this chapter.

**The Business Case**

Software architecture is a field of study that is characterized by an unusual diversity of views and understandings of some fundamental concepts. As we have already mentioned, a quick search of the internet will yield many definitions of architecture. Similarly, there is a diversity of views on the role and importance of connectors, and even whether they deserve a separate treatment from components. The reader will also find arguments (even explicitly embodied in component models such as DCOM's) that components are exclusively executable entities, which would go against much of the motivations and underpinnings of software architecture.

Simply put, imprecise and inconsistent use of poorly defined, and sometimes undefined, terms is counter to success in a highly competitive environment such as software product development. The ability to build quality products, and amass and train a skilled workforce, requires precise use of concrete terminology with specific meanings.

A specific instance of this issue would be an organization intending to hire and/or train a software architect. Without a shared technical language, hiring such an individual would be difficult and risky. Without a precise understanding of the foundational concepts in the field of software architecture, training software architects would be expensive and ultimately unproductive.

### 3.6 Review Questions

1. A question often asked of software architects is what the difference is between architecture and design. Given the definition of software architecture provided in this chapter, can you distinguish between the two?
2. What are the key differences between a software component and a software connector?
3. Can connectors simply be treated as special-purpose components? Should they?

4. Should architects and engineers be expected to accept architectural degradation as a fact of life? What, if any, dangers are inherent in doing that?
5. What is the difference between an architectural style and an architectural pattern?
6. Can multiple patterns be used to realize a style?
7. Why should architects concern themselves with the needs of the customers?

### 3.7 Exercises

1. Identify components, connectors, topology in a well known system's architecture. This can be something Web-based, something described in a publication, or even one of the examples introduced in the book so far, but for which this question hasn't been answered as part of the chapter.
  - a. How can you tell components apart from connectors?
  - b. Is the architecture descriptive or prescriptive?
2. The section that defined architectural styles provides a set of architectural guidelines corresponding to client-server systems. Select a distributed application scenario of your choice and show how you would turn these guidelines into specific design decisions. How easy are the guidelines to apply correctly? How easy are they to violate? Try to violate the 2<sup>nd</sup> guideline and discuss the immediate and potential impact on your architecture.
3. Try to solve the above problem by applying one or more of the patterns discussed in the section that defined architectural patterns. Compare this solution to the previous one. Discuss which approach was easier to apply and why.

### 3.8 Further Reading

The first explicit treatment of software architecture and the concepts that underlie it was provided by Perry and Wolf in [221]. This seminal paper introduced several definitions that have inspired those we have provided in this chapter. Several years later, Shaw and Garlan's book [259] provided their collection of definitions, summaries of several industrial and research projects in which the authors were involved, and early architectural insights from those projects. Several subsequent books on software architectures have come out since then, offering the respective authors' takes on different facets of architecture: modeling [123], evaluation [39], architectural patterns [33], product lines [25], and component-based system development [272].

A very large number of conference and journal articles accompanied these books, and several specialized venues emerged. Initially, the SIGSOFT International Software Architecture Workshop (ISAW) was the primary venue for researchers and practitioners in the field of software architecture to exchange their ideas and develop common understandings. A more narrowly focused workshop series on the Role of Software Architecture for Testing and Analysis (ROSATEA) followed soon thereafter. ISAW was eventually supplanted by the Working IEEE/IFIP Conference on Software Architecture (WICSA). More recently, the European Conference on Software Architecture (ECSA) and the International Conference on the Quality of Software Architectures (QoSA) have also emerged. The ongoing conference series on Component-Based Software Engineering (CBSE) has naturally had a significant architectural dimension. Finally, the Elsevier Journal on Systems and Software has recently introduced a regular section on software architecture.

While this wealth of books, papers, workshops, conferences, and journals has helped the field of software architecture to mature relatively quickly, it did not result in a convergence of understanding of the principal architectural concepts. One example of this lack of convergence is the use by the software engineering community of a very large and divergent collection of different definitions of software architecture, gathered by the Software Engineering Institute (<http://www.sei.cmu.edu/architecture/definitions.html>). While collecting all those definitions may be useful as a sort of historical record, actually relying on all of them is not a hallmark of a mature engineering field. That realization was one of the primary motivators for this book, and this chapter in particular.

## CHAPTER 4

# 4 Designing Architectures

The preceding chapters have laid the foundation for software architecture. The motivations for focusing on architectures and the benefits that result were laid out in Chapter 1. Chapter 2 positioned software architecture with respect to the major activities of software engineering. Chapter 3 took the informal notions of the first two chapters and set them on a firm basis.

So far, however, we have largely neglected the question of *how* architectures are created. Returning to the analogy of building architectures, simply having a set of robust power tools and a lofty vision for a skyscraper, for example, is not a fully adequate basis for creating a 50-story building that successfully houses businesses, provides the base for a television broadcast tower, and which effectively integrates with a city's electrical, water, data, and wastewater infrastructures. The small matter of "design" stands between realization of the vision and the raw materials and tools. The design of a skyscraper is the product of a cadre of architects and engineers who labor to meet all the goals for the building while simultaneously satisfying all the constraints placed upon it, and upon them.

But how are designs such as this created? How are engineers and architects taught to approach the problem?

For many serious engineers and building architects design is viewed as something that cannot be taught as a method. Rather, students are apprenticed: one "sits by the feet of the master" and hopefully by some mysterious process of osmosis the student eventually acquires some smidgen of the master's ability. For others, the ability to design is simply something one is either born with or not. We disagree with both these views. First, as human beings we all have the ability to design; we are all innately designers, and in fact engage that ability regularly in our daily lives, from cooking to decorating to painting to writing. It is just how we are made. Second, design is subject to rigorous, methodical examination, like any other endeavor – there is nothing about it which renders it incapable of study. The outcome of such study is a set of approaches and techniques for designing which can be described, taught, applied,

evaluated, and refined. Examination of existing designs helps identify good strategies for tackling various kinds of problems and helps develop a sense for associated costs and qualities. At a very minimum students can be taught the use of design tools and simple design methods. Be assured, however, that study of design methods does not imply that there is no place, or need, for creativity. Far from it; one outcome of disciplined study of design is a focusing of design effort and creativity on those aspects of problems which demand it.

The goal of this chapter, therefore, is to set forth a variety of approaches for designing, helping the student learn how to design software systems. We begin with considering some basics of design processes and then move on to foundational conceptual tools; easy to understand, but perhaps hard to apply. To provide a more concrete grip on the task we then examine in detail a variety of techniques that exploit the most useful software design tool of all: refined experience. This discussion briefly reviews the subject of domain-specific software architectures, as introduced in Chapters 1 and 2, putting this particular technique in context with others. The chapter then introduces a wide gamut of architectural patterns and styles that capture and exploit the experience of preceding designs. The section concludes with a discussion of design recovery: the process of making the design of an existing system explicit in such a way that it becomes useful in the tasks of extending or modifying that system, or using that architecture as a basis for a new system. This of course reinforces one of this text's primary themes: architecture is the centerpiece of system development and evolution; while designing the architecture is the focus of this chapter, extending and maintaining the architecture is something that occurs throughout a system's lifespan.

When refined experience proves inadequate or is unavailable for solving a new design problem, we describe a variety of techniques for dealing with such design challenges. The techniques presented draw from industrial product design, building architectures, and other sources, as well as software engineering.

The chapter concludes by briefly returning to the topic of design processes, tying the whole discussion together. Since this is a long chapter, with a multitude of techniques and approaches described, this section helps to put all the details into perspective.

A designer may come to a problem from many starting points: with no prior relevant experience, with much directly relevant experience, or with a goal of simply recovering a design. This chapter provides insights for each.

#### Outline of Chapter 4

- 4 Designing Architectures
- 4.1 The Design Process
- 4.2 Architectural Conception
- 4.2.1 Fundamental Conceptual Tools
- 4.2.2 The Grand Tool: Refined Experience
- 4.3 Refined Experience in Action: Styles and Architectural Patterns
- 4.3.1 Domain Specific Software Architectures
- 4.3.2 Architectural Patterns
- 4.3.3 Introduction to Styles
- 4.3.4 Simple Styles
- 4.3.5 More Complex Styles
- 4.3.6 Discussion: Patterns and Styles
- 4.4 Architectural Conception In Absence of Experience: "Unprecedented" Design
- 4.5 Putting it All Together: Design Processes Revisited
- 4.5.1 Insights from Requirements
- 4.5.2 Insights from Implementation
- 4.6 End Matter
- 4.7 Review Questions
- 4.8 Exercises
- 4.9 Further Reading

## 4.1 The Design Process

The typical assumption of software design is that the process can proceed in the general manner of architectural design or engineering design, which can be summarized [145] as consisting of the following four stages:

1. Feasibility stage: identifying a set of feasible concepts
2. Preliminary design stage: selection and development of the best concept
3. Detailed design stage: development of engineering descriptions of the concept
4. Planning stage: evaluating and altering the concept to suit the requirements of production, distribution, consumption and product retirement.

Of these processes, Jones comments ([145], page 24): "... designing begins (stage 1) by the taking-in of information. From this a set of alternative arrangements for the design as a whole is quickly derived. Stage 2 is to select one of these alternatives for further development. When this design has reached the point of satisfying the chief designer the work is split up for detailed design by many people working in parallel (stages 3 and 4)."

The reader will quickly recognize that this approach to design is completely consistent with common, broader notions of software engineering processes, such as the waterfall and spiral models of development. It is similarly consistent with more specific approaches to design, such as the Unified Process, Jackson System Development, and Microsoft's Code Complete. Such universal use indicates that it is a very effective strategy in many, many situations.

The viewpoint represented by this process so pervades the software development world that it is hard to realize that the use of this process represents a choice – that indeed other approaches are possible. This is an important recognition because the standard approach does not always work. Even in those situations where it does work, it may not yield the best results. At a minimum designers must be aware of some of the conditions under which the traditional approach is likely to be insufficient.

We will consider first the conditions under which this process may not work, and then briefly consider some alternative strategies.

- More than anything else, success of the standard process is predicated on the success of the first step: identifying a set of feasible concepts for the overall structure of the system.. If the designer is unable to produce such a set, progress stops.
- While not intrinsically part of the standard approach, in history and in typical current practice the first step (or two) is performed by an individual. As problems and products increase in size and complexity, the probability that any one individual can successfully perform the first steps decreases. Merely saying that those steps should be performed by a design team does not resolve the issue: the existence of a team generates new problems. These problems can be resolved, or at least mitigated, but honesty demands that their existence be explicitly acknowledged.
- In a similar vein, the standard approach does not directly address the situation where *system* design is at stake, i.e. when relationships between a *set* of products is at issue. The issue is again complexity. As complexity of the problem increases, the likelihood of an individual successfully performing the first step of the typical process decreases.

The common thread in these remarks is complexity of the application being designed. As complexity increases or, as we shall see later, the experience of the designer is not sufficient for the challenge, alternative approaches to the design process must be adopted. As Jones puts it, "... the principle of deciding the form of the whole before the details have been explored outside the mind of the chief designer does not work in novel situations for which the necessary experience cannot be contained within the mind of one person."

The good news is that there are many design strategies to choose from – essentially they are process models applied at the level of design:

- Standard: the linear model described above;
- Cyclic: as problems or infeasible approaches are identified in stages 2-4 of the standard model, the process reverts to an earlier stage;
- Parallel: after stage 1 of the standard model, independent alternatives are explored in parallel; at suitable times selection is made between the identified viable alternatives. A related strategy is to parallelize at stage 1: multiple independent attempts at design are initiated, with no dependencies between them;
- Adaptive ("lay tracks as you go"): the design strategy to follow in the next stage of the design activity is decided at the end of a given stage, based upon insights gained during that stage;
- Incremental: design at each stage of development is treated as a task of incrementally improving whatever design or previous product exists after a preceding stage.

Sensible management of the design process also yields another "strategy": the process is observed as it proceeds and the methods and approach used are modified as needed to focus on the best strategy and to avoid unpromising developments.

Now that we have identified conditions under which the standard approach to design does not work, as well as identifying some alternative approaches, we will now focus on the critical first step of design: identifying a candidate set of feasible concepts.

## 4.2 Architectural Conception

The standard approach to architectural and engineering design says that the first major step consists of identifying a feasible set of "alternative arrangements for the design as a whole", then choosing one of those arrangements, and then proceeding to refine and elaborate it. What the standard approach does not tell, however, is *how* to identify that set of viable arrangements – or even one viable arrangement.

A facile answer to the question is to simply state, "Apply the fundamental design tools of software engineering: abstraction and modularity." While the utility, even the necessity, of such intellectual tools is unquestionable, they are only tools. As very basic tools – principles, really – one must decide where and how to wield them. One can carve with those knives, but to what design?

An equally facile answer is just to say “inspiration”. Creative inspiration is needed, to be sure, but it is not a reliable magic wand to be blithely waved over a complex design challenge. A more effective strategy is to minimize and isolate those parts of a design for which creative inspiration is required, and to apply more prosaic and predictable techniques elsewhere. In other words, focus the creative efforts. Still, however, one has to know where creativity is required, and where it is not.

A common, effective, and appropriate answer to the question of how to identify a feasible set of “alternative arrangements for the design as a whole” is applying experience. As the remainder of this chapter will reveal, this is not a shallow answer to the problem. There is substantial sophistication to the use of “experience”. It is not foolproof and does not always suffice – but treatment of these issues comes later.

We proceed by first discussing the most basic design tools of software engineering, and then begin an extended discussion of how the lessons of experience may be used to tackle new design problems.

#### 4.2.1 Fundamental Conceptual Tools

The most basic design tools are separation of concerns, abstraction, modularity, and other “first principles of software engineering” such as anticipation of change and design for generality. As noted above, however, they are hard to apply “straight out of the box”; fortunately it is usually not necessary to do so, as the rest of the chapter will show. Since these concepts are familiar, we provide only a brief discussion.

##### Abstraction and the Simple Machines

Abstraction is the selection of a set of concepts to represent a more complex whole. One view of this definition sees abstraction as a process that moves “upwards”, from details to summarizing concepts. As it relates to design, however, abstraction is usually employed as a tool to be used when moving “downwards”: a set of concepts is chosen to allow discussion of an idea – an arrangement of abstract parts that (hopefully) constitutes a solution, though still at a high level. The design then moves further downwards, as the concepts of the abstraction are reified into more concrete structures – a more complex whole. Ultimately the reification process ends with the production of source code. While “refinement” or “deduction” might be more accurate and appropriate terms for this activity, “abstraction” is often used because the intent from the outset is to create source code for which the abstraction is an accurate and widely useful characterization.

Terminology:

**Abstraction:** “The act or process of separating in thought, of considering

##### Abstraction, Reification, Deduction, and Induction

a thing independently of its associations; or a substance independently of its attributes; or an attribute or quality independently of the substance to which it belongs.” [1]

1855 BAIN Senses & Intel. (1864) III. iv, §17. 606 The first in order of the scientific processes is Abstraction, or the generalizing of some property, so as to present it to the mind, apart from the other properties that usually go along with it in nature.

**Reification:** “The mental conversion of ... [an] abstract concept into a thing.” [3] Otherwise known as thingification ©

**Deduction:** “The process of deducing or drawing a conclusion from a principle already known or assumed; spec. in Logic, inference by reasoning from generals to particulars; opposed to INDUCTION.” [3]

1862 BUCKLE Civiliz. (1869) III. v. 291 By deduction we descend from the abstract to the concrete.

**Induction:** “The process of inferring a general law or principle from the observation of particular instances (opposed to DEDUCTION, q.v.)” [3]

The question remains, though, what concepts should be chosen at the outset of a design task? One good answer, and one that helps support the use of the term “abstraction” is, “Search for a simple machine that serves as an abstraction of a potential system that will perform the required task”.

The simple machines of software design are many. For instance, what kind of simple machine makes a spreadsheet program? It is “just a graph of relationships, and when one node is changed, the relationships are all re-evaluated to bring everything back into sync.” What makes up a parser? “Essentially, it is just a push-down automaton.” How does fax machine software work? “At core, it is basically just a little state machine” How does an avionics system work? “You just read all the sensors, calculate the control laws, write values out to the displays and actuators, and then do it all over again.”

While these answers may seem trivial and inadequate – and they are in many ways – the point is that they provide a plausible first conception of how an application might be built. That is, they provide the first clues into designing a system’s architecture.

Every application domain has its common simple machines. The “commonness” of these simple machines reflects, of course, experience in designing applications within those domains. Some examples are shown

in Figure 4-1. Choice of a simple machine can enable further exploration of the feasibility of that design concept.

Domain	Simple Machines
Graphics	Pixel arrays Transformation matrices Widgets Abstract depiction graphs
Word processing	Structured documents Layouts
Process control	Finite state machines
Income Tax Software	Hypertext Spreadsheets Form templates
Web pages	Hypertext Composite documents
Scientific computing	Matrices Mathematical functions
Banking	Spreadsheets Databases Transactions

Figure 4-1. Common simple machines

#### Choosing the Level and Terms of Discourse

Whether or not the approach of attempting to identify simple machines is adopted, any attempt to use abstraction as a tool must choose a field of discourse, and once that is chosen, must choose the terms used in discourse. Often the two choices are virtually inseparable.

The linear, or standard approach, to architectural concept formation demands that the initial subject of discourse be that of the application as a whole. For example, the old technique of step-wise refinement begins at that "level".

Two alternatives exist, however. The first is to choose to work, initially, at a level lower than that of the whole application. That is, the subject of discourse might be something that is optimistically assumed to be a "part of" a solution to the larger problem. Design is performed at that level in the hope that once several such sub-problems are solved they can be composed together to form an overall solution, where their means of composition does not impinge upon their internal structure. Success with this approach need not demand great foresight; sometimes just whittling away at parts of a problem makes later tackling of the overall problem easier. Good foresight certainly helps, of course.

The occasion when this approach is particularly appropriate is when there exists a body of pre-existing components which are available for reuse in the development of a new application. (N.B. this is almost *always* the case!) Thorough understanding of what those components are capable of, and how they may be composed, can provide critical insights into how the whole application should be structured so as to enable the potential reuse.

The other alternative is to choose to work, initially, at a level *above* that of the desired application. In some cases this may mean solving a more general problem. A good example of where this has worked out well is in handling complicated input to programs. Rather than building a custom component for processing an application's simple, restricted user input language, it can be very effective to employ a generic parser tool. Though the parser may end up being far more powerful than what the specific application requires, the maturity of technology development in that domain, coupled with an abundance of reusable packages embodying that technology, will likely result in a smaller, faster, off-the-shelf component being used.

In other cases this may simply mean understanding the core issues of an application in a more fundamental way. To use a physical example, building a guitar may suggest thinking about choosing strings, wood for the fingerboard, side, top, bridge, and so on. Moving up a level of abstraction, however, would involve thinking about the physics of vibrating strings, wave propagation, and whatnot (see, for example [301]). The benefit would be to identify in advance what the key design factors are.

To use a software example, consider the challenge of designing an application to help in the preparation of income tax returns. For any given year the nation's tax laws determine what information must be reported, what calculations must be done, and how the information must be reported on various forms. Publications from the taxing authority provide instructions and explanations. A custom application could, of course, be designed to perform those functions as required. But if the problem is reconsidered at a higher, more abstract level, it can be formulated as a spreadsheet problem coupled with a formatting (text-layout) problem coupled with hypertext. The spreadsheet includes within it the particular formulas required in a given year. The text layout can be viewed in a similarly generic way, with rules specifying the particular layout required for a particular year. Hypertext associates instructions with the portions of the forms to which the instructions apply. Built in this way (i.e. using a generic spreadsheet engine, a generic form layout engine, and a hypertext engine) a tax software application can be created and updated efficiently from year to year, enabling a profitable business.

### Separation of Concerns

Separation of concerns is the subdivision of a problem into independent parts. For instance, the visual interface that a customer sees at a bank's automatic teller machine is independent from the logic used to control operation on that customer's accounts. If the concepts at issue are genuinely independent, then using this technique is straightforward. The difficulties arise when the issues are either actually or apparently intertwined.

When such interrelationships are found their causes should be identified. Sometimes interrelationships may be present just because of use, or abuse, of language. For example, a single, common word such as "account" may be used to describe what are in-fact different entities in different parts of an application. In other cases concepts may be intertwined because of (past or prospective) solution efficiency. For example, the presence of numeric keys in user records may simply reflect prior database implementation strategies, and not be intrinsic information about the user.

A primary example of separation of concerns at work in software architecture is the separation of a system's structure into components (loci of computation) and connectors (loci of communication). This separation reflects the independence of the issues and is at the heart of the chapter on connectors. The myriad of details and concerns addressed in that chapter reveals that, like many applications of the principle, numerous tradeoffs and alternatives must be considered.

Separations of concerns frequently involves many tradeoffs; total independence of concepts may not be possible. The designer is thus left with the substantial obligation of assessing performance, cost, appearance, or functional tradeoffs between competing conceptions.

## 4.2.2 The Grand Tool: Refined Experience

While the intellectual tools of abstraction and separation of concerns are of undeniable use in the process of designing an architecture, in and of themselves they provide scant guidance to the designer. Experience can be a masterful teacher, however, and provide the guidance necessary to wield the basic tools in effective fashion. Raw experience by itself, though, does not provide the mature guidance that enables effectively tackling new problems. Experience must be reflected upon and refined to the point where the designer understands the essential issues and lessons from prior work, enabling judicious choice of context-appropriate techniques.

The lessons from prior work include not only the lessons of successes, but also the lessons arising from failure. In either case it is only reflection that can indicate the root causes for the success or failure, and hence the critical knowledge that can be carried forward. (This is not to say that every failure has the seeds of valuable technical advice. Regrettably too many projects fail for reasons independent of technology.) Lessons from prior work need not only come from one's own experience, of course. One virtue of reading widely in a technical field or attending technical conferences is to benefit from the experiences of others. There is no virtue in reinventing wheels, broken or otherwise.

When valuable technical experience is possessed, however, substantial efficiencies result. Experience can provide that initial feasible set of "alternative arrangements for the design as a whole" called for at the beginning of Section 4.1. One need not devote valuable design time to topics for which one already has a validated solution in hand. Similarly, communication between development team members is enhanced: when others have experience with the same or similar pre-existing systems, it is easier to describe use of or modifications to an established approach, as compared to conveying a completely new concept.

Applying established approaches is not an entirely risk-free strategy however. Once one has a favorite hammer, everything starts to look like a nail. Pursuing such a strategy may yield a working application, but can easily yield one which is seriously deficient in some respect or at least be suboptimal. Not only are the benefits of previous systems imported by reusing an approach, but so are the limitations. Innovation is certainly inhibited by always mindlessly following one's standard approach. That said, it is nonetheless clear that refined experience is indeed the Grand Tool for designers to apply in creating new applications.

### Silver Bullets and other Misfires

Software engineering literature is replete with "sure fire" approaches to design – tools and techniques that are assured to always work and provide that needed solution. Some of these mistaken approaches to design confuse a notation or language with a design method. UML, for instance, is a notation, not an approach. So, too, is Java. Other approaches confuse a tool or technology with a design method. Thus some have said that CORBA provides all the needed guidance for building robotic systems; others have assured us that rule-based "expert" systems are all we need. Most assuredly, there is no magic potion, and an adequate approach to design problems demands care, thought, creativity, discipline, experience, and method.

The software designer of the 21<sup>st</sup> century has a wide basis of experience from which to draw. Reflection on the development of thousands of

systems has yielded a wide variety of approaches and lessons, ranging from broadly encompassing domain-specific architectures to simple programming language-level design patterns. The following section presents lessons from this experience base in considerable detail.

### 4.3 Refined Experience in Action: Styles and Architectural Patterns

The distilled architectural wisdom that has arisen from a vast body of experience comes in many shapes and flavors. As a whole, we are treating them under the rubric of styles and patterns. As introduced in Chapter 1, the notion of architectural styles is an ancient one, dating back at least to Vitruvius. Styles are designed to capture knowledge of effective designs for achieving specified goals within a particular application context. For building architecture the combination of goals and context might be providing a home for a single family in a Mediterranean climate using stone and tile as principal building materials. The correspondingly appropriate style might be a single-story villa. For software the goals and context might be providing a secure instant messaging system to operate between remote sites of a global company; the appropriate style might be client-server.

Patterns and styles can be characterized for large problems as well as small. Again, with regard to buildings one can characterize a pattern for determining the appropriate overhang of a tiled roof over an entryway; similarly one can characterize a (much more complicated) pattern for provision of elevator service in a ninety-story skyscraper. So it is with software architecture: patterns and styles have been developed that are appropriate for small applications as well as large and complex ones.

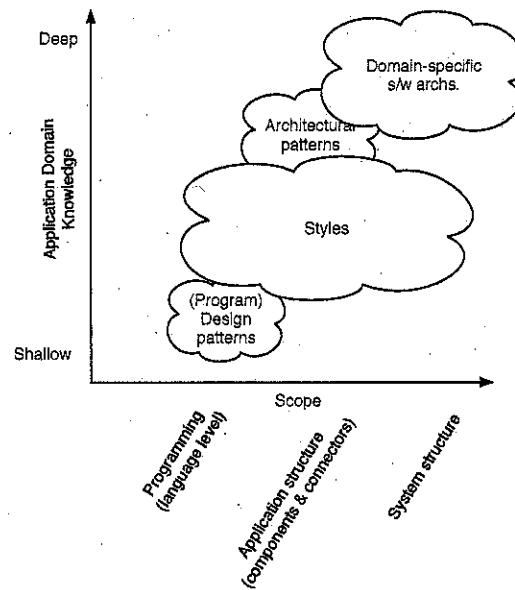
Not surprisingly the lessons of experience in software architecture have arisen from several different software development communities – each has its own contribution to make. Unfortunately this has resulted in a variety of terms for characterizing this experience, not all of which describe distinct concepts. As an aid to teasing out the various issues and as a means to provide structure for the rest of this section, we have summarized the main types of architectural styles and patterns in Figure 4-2

The x-axis of this figure refers to the scope of applicability of the body of knowledge – the domain of discourse. For instance, design patterns exemplified by those presented in the book by Gamma, et.al.[85], are focused on the programming of object-oriented solutions to program design problems. Such patterns are inapplicable to enterprise-level system design, which is at the other end of the x-axis.

The y-axis reflects the amount of domain knowledge represented by (or encoded within) the body of knowledge. Program design patterns are shown at the shallow end of this scale, reflecting that they are very generally applicable, and are not restricted to use within a particular application domain. At the other end of the scale are domain-specific software architectures. Such styles are applicable to the design of very large applications and concomitantly encode substantial knowledge about the design of applications within a domain. Thus for instance a domain-specific software architecture for retail banking might specify all major parts of the application; it is unlikely, however that such a structure would be appropriate for any other kind of application apart from retail banking.

The diagram has fuzzy boundaries, however, and should only be taken as a rough guide. Programming languages exist at many levels of abstraction; applications range from very simple to extraordinarily complex. The “scope” axis should not, therefore, be taken as genuinely linear or fully ordered. The “concept clouds” in the diagram similarly have fuzzy boundaries. What one architect may term an “architectural pattern” might be called a style by another.

The following sections will bring a little more precision to the discussion. While the topic of domain-specific architectures will be dealt with at substantial length in a later chapter, we begin the following exposition by a brief consideration of such architectures, as they are a powerful way of exploiting experience in the task of developing the architecture for a new system. We then consider architectural patterns and styles at length. These topics were introduced and defined in the preceding chapters; here a wide variety of specific instances are presented. This chapter does not include any further discussion of program design patterns. As Figure 4-2 indicates, such patterns deal with concepts at the level of programming languages, and object-oriented languages in particular. As such they offer little guidance to the architect seeking to identify a feasible set of “alternative arrangements for the design as a whole”. (They do, of course, offer significant guidance to a programmer tasked with implementing a chosen architecture in an object-oriented language, but that is not the topic of this chapter.)



**Figure 4-2.** Domain knowledge vs. Scope in showing the relationship between styles and patterns. Beware! The boundaries between the concepts are not precise.

### 4.3.1 Domain Specific Software Architectures

Domain-specific software architectures (DSSAs) encode substantial knowledge about how to structure complete applications within a particular domain. A useful operational definition of DSSA is the combination of a *reference architecture* for an application domain (as defined in Chapter 3), a library of software components for that architecture containing reusable chunks of domain expertise, and a method of choosing and configuring components to work within an instance of the reference architecture [114]. As such, a DSSA represents the most valuable type of experience useful in identifying a feasible set of “alternative arrangements for the design as a whole”.

In terms of our familiar building analogy, DSSAs are akin to the generic design of tract homes, i.e. home designs which are instantiated dozens or hundreds of times to yield individual homes in a housing development. Such homes are not identical to one another; typically they will vary in terms of cabinetry, banister styles, colors, carpet, roofing material, and

such. They will be same, though, with respect to the floor plan, the location of the windows, and with regard to all major structural elements. The contractor for an individual home knows how to instantiate the generic plan in light of the consumer’s specific preferences and choices to yield a very cost-effective structure that nonetheless is somewhat personalized.

The extended example of software for consumer electronics presented in Chapter 1 serves as an illustration of a DSSA. (While this example was presented there as an illustration of product families, the two concepts are closely related. This relationship is carefully explored in Chapter 15.) Different consumer electronics applications can be created by “parameterizing” or specializing the core architecture. These specializations may represent adding new, unprecedented components into a television’s architecture, for instance, but where those additions are performed on parts of the architecture identified in advance as places for such extensions to occur.

The difficulty with DSSAs, of course, is that since they are specialized for a particular domain they are only of value if one exists for the domain wherein the engineer is tasked with building a new application. While this may make it sound as though DSSAs are rare, the contrary is true. Companies tend to develop multiple applications within a particular area of expertise. This expertise manifests itself in strong similarities in structure between one product from the company and another. These similarities, and the rationale for them, is the basis of a DSSA. What is unfortunately true of such situations, however, is that frequently the common structure – the DSSA – is never written down, but remains latent in the minds of the company’s engineers.

Since Chapter 15 explores DSSAs and product families in substantial detail, further discussion of these concepts is deferred. The reader should remember, however, that DSSAs are the pre-eminent means for maximal reuse of knowledge and prior development and hence for developing a new architectural design in an established domain.

### 4.3.2 Architectural Patterns

Architectural patterns are akin to DSSAs, but applied within a much narrower scope. Hence they represent significant reuse of experience, but help you less fully. We repeat here the definition from Chapter 3:

**Definition.** An architectural pattern is a set of architectural design decisions that are applicable to a recurring design problem, and parameterized to account for different software development contexts in which that problem appears.

In the sections below, we sketch three very simple examples: State-Logic-Display, Model-View-Controller, and Sense-Compute-Control.

#### State-Logic-Display (a.k.a. Three-tier)

The example used in Chapter 3 to illustrate this definition is the familiar “three-tier architecture”, which is commonly employed in business applications where there is a (usually large) data store behind a set of business logic rules, and that set of functions is accessed by user interface components. This pattern, also known as State-Logic-Display, has been popular since it maps nicely to a distributed implementation in which communication between the components is by a remote procedure call. Figure 4-3 shows the pattern, redrawn in a different orientation from that used in Chapter 3.

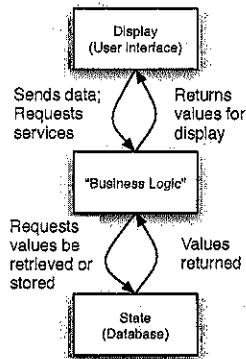


Figure 4-3. Canonical structure of State-Logic-Display Architectures.

In business applications the data store is usually a large database server; the business logic component may implement, e.g., some banking transaction rules, and the display component be a relatively simple component for managing interaction with a user on a desktop PC. Multiplayer games also map nicely to this architecture, wherein the “business logic” component implements the play rules of the game and the data store maintains the game state. Multiple players can simultaneously play the game wherein each user has his own display component. Many web-based applications can be approximately characterized as three-tier architectures, where the display component is the user’s web browser, the business logic component is the software on the web site (web server plus application specific logic) and the data store is a database accessed by the web server on a local host. This characterization of web applications is not entirely fair, however, as communication between the display component (browser) and the business logic component (web server) is

not by means of a remote procedure call, but rather by the HTTP protocol, which does not necessarily maintain a connection between the two components in between interactions.

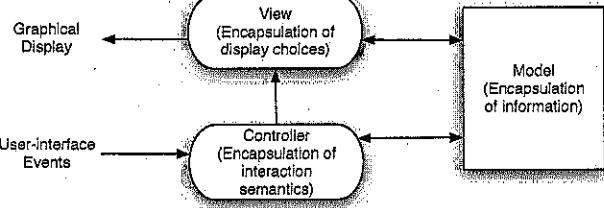
#### Model-View-Controller (for Graphical User Interfaces)

Since its invention in the 1980’s, the model-view-controller (MVC) pattern has been a dominant influence in the design of graphical user interfaces. While MVC certainly is applied at the low levels of program design, and thus could be classified in the “design patterns” category (and hence omitted from our discussion here), it can also be viewed as providing a structure for applications at a higher level.

The objective of the pattern is to promote separation, and thus independent development paths, between information manipulated by a program and depictions of and user interactions with that information. The simple idea is shown in Figure 4-4. The model component encapsulates the information used by the application; the view component encapsulates the information chosen and necessary for graphical depiction of that information; the controller component encapsulates the logic necessary to maintain consistency between the model and the view, and to handle inputs from the user as they relate to the depiction.

The notional interactions between these components is as follows (variations exist in the practice). When the application changes a value in the model object, notification of that change is sent to the view so that any affected parts of the depiction can be updated and redrawn. Notification also typically goes to the controller as well, so that the controller can modify the view if its logic so requires. The View may query the Model for additional data needed for the display. When handling input from the user (such as a mouse click on part of the view), the windowing system sends the user event to the controller; the controller may query the view for information to assist in determining what action to take. The controller then updates the model object in keeping with the desired semantics. Then, of course, if the model object changes values it must notify the view and controller so that the user interface can be updated, and so the cycle of interactions continues.

While Figure 4-4 shows three distinct components, from the description above of their interactions it is clear that there is often a very close coupling between the actions of the view component and the controller component. In many cases therefore, the view and controller components are merged; such is the case with the architecture of Java’s Swing framework.



**Figure 4-4.** Notional Model-View-Controller Pattern

At a much higher level of abstraction than programming, the MVC paradigm can be seen at work in the WWW. Web resources correspond to the model objects; the HTML rendering agent within a browser corresponds to the viewer; the controller in the simplest case corresponds to the code which is part of the browser that responds to user input and which either causes interactions with a web server, or which modifies the browser's display in some manner. In the more complicated situation the controller would also encompass code uploaded from a server which governs user interaction with the display, such as Javascript uploaded as part of a web page, or code on the server that determines what representation of the resource to transmit to the browser.

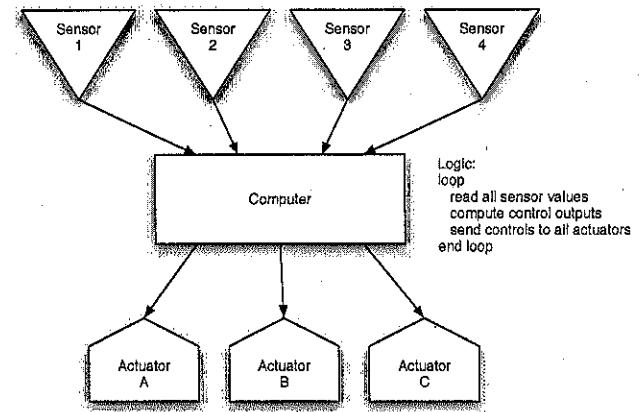
MVC has been the subject of much work, and a variety of references are available discussing the details of several different implementation approaches. MVC has also inspired the development of other, related architectural patterns, such as Presentation-Abstraction-Controller (PAC). Detailed citations are provided at the end of the chapter.

#### Sense-compute-control (a.k.a. sensor-controller-actuator)

The Sense-Compute-Control (SCC) pattern is typically used in structuring embedded control applications. This may range from simple devices such as found in kitchen appliances to sophisticated systems used in automotive applications or robotic control. The basic idea is illustrated in Figure 4-5. A computer is embedded in some application; sensors from various devices are connected to the computer and may be sampled to determine their value. Also attached to the computer are hardware actuators. By sending a signal to such devices the computer may, e.g. open a valve, lower flaps, or turn off a light, and hence control the system.

The architectural pattern is simply one of cycling through the steps of reading all the sensor values, executing a set of control "laws" or functions, and then sending outputs to the various actuators. Typically such a cycle is keyed to a clock, where the frequency of the clock "ticks" may be keyed to the maximum rate at which the sensors' values may

change, or the sensitivity of the actuators to varying inputs on their input control lines. Note that there is implicit feedback in such applications, via the external environment. That is, the typical situation is that by changing one of the actuators, something will change in the external environment that one of the sensors will ultimately detect, and hence cause a change in its value.



**Figure 4-5.** Sense-Compute-Control. Different shaped boxes are used to indicate the different types of devices present in the system.

A simple flight control application can serve to make these ideas concrete. We will use the example of software controlling a notional lunar excursion module (LEM) to the surface of the moon, illustrated in Figure 4-6.

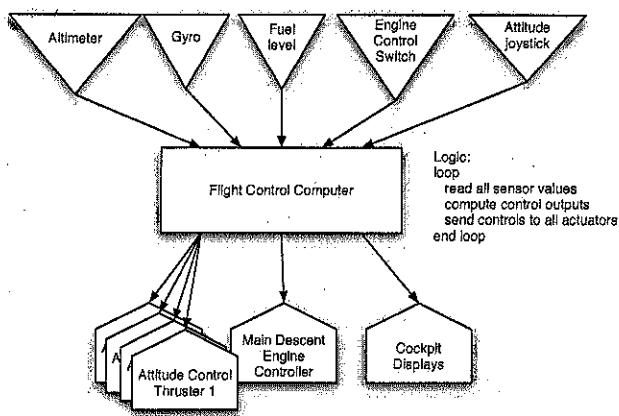


Figure 4-6. Sense-compute-control applied to a lunar lander

In this example there are five sensors on board the spacecraft; the altimeter (presumably radar) senses the altitude above the surface of the moon; the gyro provides information on the x-y-z axis orientation of the craft; the fuel level indicates the remaining fuel on board; the engine control throttle indicates to the computer the pilot's desired setting of the descent engine's thrust (e.g. 75% throttle); the joystick indicates the pilot's inputs for orienting the spacecraft. The diagram shows six actuators: four attitude control thrusters, the main descent engine controller, and the cockpit displays.

As the craft approaches the surface, the sensors will provide to the computer information on the LEM's altitude, attitude, fuel remaining, and the pilot's control inputs. The flight control computer will process its control laws, computing values to be sent to the various actuators to control the descent engine, the attitude control thrusters, and update the cockpit displays. From changes in the altitude the computer could determine, for example, the descent rate, and display that to the pilot. Based upon the pilot's judgment, he could increase the throttle to slow the descent or decrease the throttle and allow the lunar gravity to increase the descent rate.

Depending on the system designer's choices, a variety of control strategies could be programmed into the flight control computer. The scenario sketched above reflects the strategy applied in the Apollo landings. A fully automated landing sequence could also be programmed, in which the software would determine the optimal descent engine and attitude control

thruster settings, based upon the altitude and attitude of the craft. From the standpoint of the software's architecture, these different strategies are all the same: at each cycle of the loop the software reads the current sensor values, computes the desired settings for the actuators, and sends those values to the actuators.

### 4.3.3 Introduction to Styles

Architectural styles are a primary way of characterizing lessons from experience in software system design. As such, they can be a key element in developing initial or detailed conceptions of a software system's architecture. As Figure 4-2 indicates, architectural styles are broadly applicable: they can be useful in determining everything from subroutine structure to top-level application structure. Styles, as used here and as seen in contrast with the architectural patterns of the preceding section, reflect less domain knowledge than architectural patterns, and hence are more broadly applicable. Keep in mind however, that the boundaries between these concepts are not precise.

Chapter 3 introduced architectural styles in some detail, and presented the following definition:

**Definition.** An architectural style is a named collection of architectural design decisions that (1) are applicable in a given development context, (2) constrain architectural design decisions that are specific to a particular system within that context, and (3) elicit beneficial qualities in each resulting system.

Accordingly, as styles are presented in this section we shall indicate the decisions and constraints comprising the style, as well as the beneficial qualities induced by these choices.

Styling with Perry and Wolf (from [221])

"The notion of architectural style is particularly useful from both descriptive and prescriptive points of view. Descriptively, architectural style defines a particular codification of design elements and formal arrangements. Prescriptively, style limits the kinds of design elements and their formal arrangements. That is, an architectural style constrains both the design elements and the formal relationships among the design elements. Analogously, we shall find this a most useful concept in software architecture."

Of extreme importance is the relationship between engineering principles and architectural style (and, of course, architecture itself). For example, one does not get the light, airy feel of the perpendicular style as exemplified in the chapel at King's College, Cambridge, from Romanesque engineering. Different engineering principles are needed to move from the massiveness of the Romanesque to lightness of the

perpendicular. It is not just a matter of aesthetics. This relationship between engineering principles and software architecture is also of fundamental importance.

Finally, the relationship between architectural style and materials is of critical importance. The materials have certain properties that are exploited in providing a particular style. One may combine structural with aesthetic uses of materials, such as that found in the post and beam construction of Tudor-style houses. However, one does not build a skyscraper with wooden posts and beams. The material aspects of the design elements provide both aesthetic and engineering bases for an architecture. Again, this relationship is of critical importance in software architecture.

Thus, we find in building architecture some fundamental insights about software architecture: multiple views are needed to emphasize and to understand different aspects of the architecture; styles are a cogent and important form of codification that can be used both descriptively and prescriptively; and, engineering principles and material properties are of fundamental importance in the development and support of a particular architecture and architectural style."

"If architecture is a formal arrangement of architectural elements, then architectural style is that which abstracts elements and formal aspects from various specific architectures. An architectural style is less constrained and less complete than a specific architecture. For example, we might talk about a distributed style or a multi-process style. In these cases, we concentrate on only certain aspects of a specific architecture: relationships between processing elements and hardware processors, and constraints on the elements, respectively.

Given this definition of architecture and architectural style, there is no hard dividing line between where architectural style leaves off and architecture begins. We have a continuum in which one person's architecture may be another's architectural style. Whether it is an architecture or a style depends in some sense on the use. For example, we propose in [another section of this article] that architectural styles be used as constraints on an architecture. Given that we want the architectural specification to be constrained only to the level desired by the architect, it could easily happen that one person's architecture might well be less constrained than another's architectural style.

The important thing about an architectural style is that it encapsulates important decisions about the architectural elements and emphasizes

important constraints on the elements and their relationships. The useful thing about style is that we can use it both to constrain the architecture and to coordinate cooperating architects. Moreover, style embodies those decisions that suffer erosion and drift. An emphasis on style as a constraint on the architecture provides a visibility to certain aspects of the architecture so that violations of those aspects and insensitivity to them will be more obvious."

The following pages provide an overview of a broad range of architectural styles. The styles chosen for presentation were selected on the basis of reflecting a diversity of approaches, commonality of use, and being a part of the common vocabulary of software architects. Sufficient detail is presented so that the reader can appreciate the essence of each style and the situations for which it is appropriate. While this chapter does not present a comprehensive catalog of styles, many of the most popular and well-known are discussed, showing the designer the kind of role that styles can play in solving design problems. Chapter 11 will explore a few more advanced styles, such as REST, in some detail. After the simpler styles have been presented here, Section 4.3.6 discusses patterns and styles in general, their use in combination, and the development of new styles.

As the following discussion will make clear, there are a variety of potential ways of classifying and organizing styles. We have chosen to present the simple styles according to the following outline:

#### Traditional language-influenced styles

- Main program and subroutines
- Object-oriented

#### Layered

- Virtual machines
- Client-server

#### Data-flow styles

- Batch sequential
- Pipe-and-filter

#### Shared memory

- Blackboard
- Rule-based

#### Interpreter

- Interpreter
- Mobile code

#### Implicit invocation

- Publish-subscribe
- Event-based

#### Peer-to-peer

Later in the chapter two slightly more complex styles are discussed: "C2" and Distributed Objects, with specific consideration of CORBA.

Other organizations would highlight other similarities and relationships between the presented styles. The above categorization should thus only be taken as one coarse-grain perspective, useful primarily in the initial introduction of the styles.

Most of the styles presented below will be illustrated in two different ways: first, by reference to a type of application for which the style is well-suited, and second by sketching a game version of the lunar lander program that was used above in illustrating the sense-compute-control (SCC) pattern. By using the same, or similar, application with each style some sharp contrasts between the styles will be evident. The game version of lunar lander differs from the SCC version in one critical respect: the environment needs to be simulated. In a real flight control application the actions of the physical universe affect the spacecraft. For instance as the lander approaches the moon, the moon's gravitational field draws the spacecraft down. Each time the sensors are read different values will appear, not due to any action of the software, but simply because of the action of gravity. In the game version the physics of the universe must be simulated. For example, upon each tick of a game clock the values of the sensors could be computed by an environment simulator, rather than read from genuine sensor devices. As you compare the various examples, please be aware that the various lunar lander games are not equivalent. The purpose of the examples is to help develop understanding of the various styles through reference to a common application context – not a common, precise, and complete requirements specification.

Though the following presentation is lengthy, the reader will most likely find it too brief to answer all the questions concerning how to use these styles. Some have complex details associated with their use which have been omitted here. Our primary objective is to illustrate a wide range of diverse styles which represent the capture of extensive experience. The material presented here can serve as an introduction to the styles, detailed instructions for the use of which must appear elsewhere.

#### 4.3.4 Simple Styles

##### Traditional Language-Influenced Styles

The two styles considered here reflect the program styles that result from the traditional use of programming languages such as C, C++, Java, and Pascal. These languages, of course, can be used to implement architectures in very different styles; discussed here are architectures that

primarily reflect the basic organizational and control-flow relationships between components provided by these imperative languages.

##### *Main Program and Subroutines*

The main program and subroutine style should be instantly familiar to anyone who has programmed in a language such as C, Fortran, Pascal, or Basic. The components are the main program and the various subroutines (a.k.a. procedures); the connectors between the components are procedure calls. For purposes of this discussion we will specifically exclude programs which use shared memory (e.g. global variables) as a means of communication from being a part of this style.

**Style:** Main Program and Subroutines (no shared memory)

**Summary:** Decomposition based upon separation of functional processing steps

**Components:** Main program and subroutines

**Connectors:** Function/Procedure calls

**Data Elements:** Values passed in/out of subroutines

**Topology:** Static organization of components is hierarchical; full structure is a directed graph.

**Additional constraints imposed:** None

**Qualities yielded:** Modularity: subroutines may be replaced with different implementations as long as interface semantics are unaffected.

##### *Rationale:*

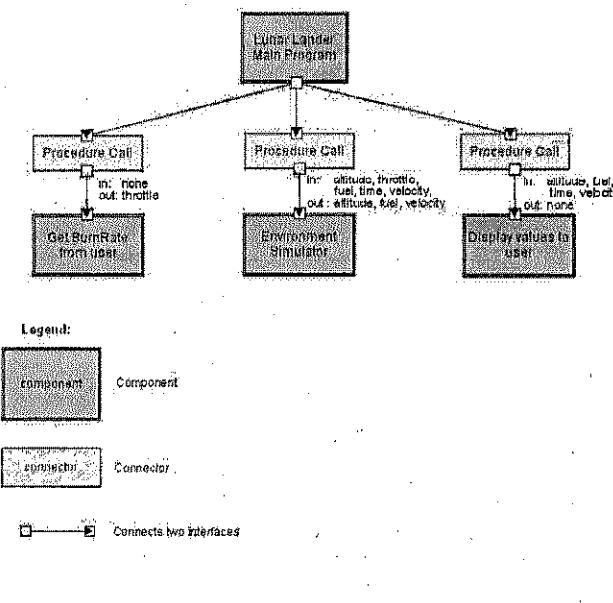
**Typical uses:** Small programs; pedagogical purposes.

**Cautions:** Typically fails to scale to large applications; inadequate attention to data structures. Unpredictable effort required to accommodate new requirements.

**Relations to programming languages or environments:** Traditional imperative programming languages, such as BASIC, Pascal, or C.

A simple version of the lunar lander game program is shown in Figure 4-7. Its design is based on the functional decomposition of the processing into repeated user interface steps (input and output) and all the processing that corresponds to simulating the environment and the actions of the spacecraft. Specifically, the main program displays greetings and instructions, then enters a loop wherein it calls the three subroutine components in turn. The first obtains the pilot's throttle-setting input. The second component primarily serves as the environment simulator, determining how much fuel is left and what the altitude and descent rate are. The only "flight control law" in this simple game is the translation of a pilot-specified throttle percentage into a volume/second fuel-flow setting (the "burn rate") to control the descent engine. The third component displays the updated state. In this game there is no clock, so one cycle through the functional processing corresponds to one clock "tick".

**Figure 4-7.** Lunar Lander: Main Program and Subroutines



#### Object-Oriented

The object-oriented style should be similarly familiar. The only “structuring” provided is that of a world of objects whose lifetime’s vary according to use. Comprehending a program structured in this manner requires understanding the numerous static and dynamic relationships between the objects.

##### Style: Object-Oriented

**Summary:** State strongly encapsulated with functions that operate on that state, as “objects”. Objects must be instantiated before the objects’ methods can be called

**Components:** Objects (a.k.a. instance of a class)

**Connector:** Method invocation (calls of functions to manipulate state)

**Data Elements:** Arguments to methods

**Topology:** Can vary arbitrarily; components may share data and interface functions through inheritance hierarchies.

**Additional constraints imposed:** Commonly: shared memory (to support use of pointers), single-threaded.

**Qualities yielded:** Integrity of data operations: data only manipulated by appropriate functions. Abstraction: implementation details hidden.

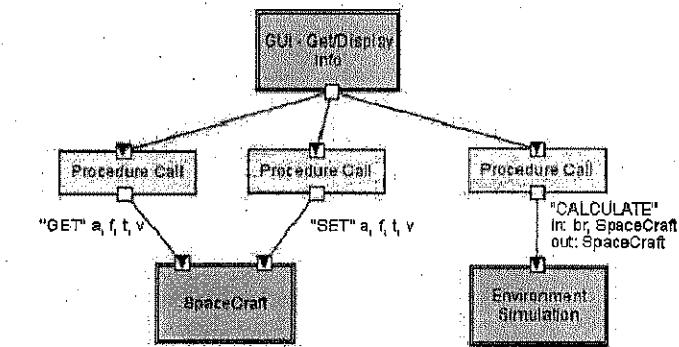
#### Rationale:

**Typical uses:** Applications where the designer wants a close correlation between entities in the physical world with entities in the program; pedagogy; applications involving complex, dynamic data structures.

**Cautions:** Use in distributed applications requires extensive middleware to provide access to remote objects. Relatively inefficient for high-performance applications with large, regular numeric data structures (e.g., scientific computing). Lack of additional structuring principles can result in highly complex applications.

**Relations to programming languages or environments:** Java, C++

**Figure 4-8.** Lunar lander in the object-oriented style



The object-oriented design of the Lunar Lander game has three encapsulations: the spacecraft, the user’s interface, and the environment (essentially a physics model that allows calculation of the descent rate). Note a contrast with the Main Program and Subroutine’s (MPS) design: here interactions with the user are handled by a single object, which performs both input and output functions. The functional decomposition of the MPS design resulted in those functions being performed by separate subroutines.  $a$  designates altitude,  $f$  denotes fuel,  $t$  denotes time,  $v$  denotes velocity, and  $br$  denotes burn rate. Some details of the object-oriented design are apparent in Figure 4-9, which is a UML characterization of the objects.

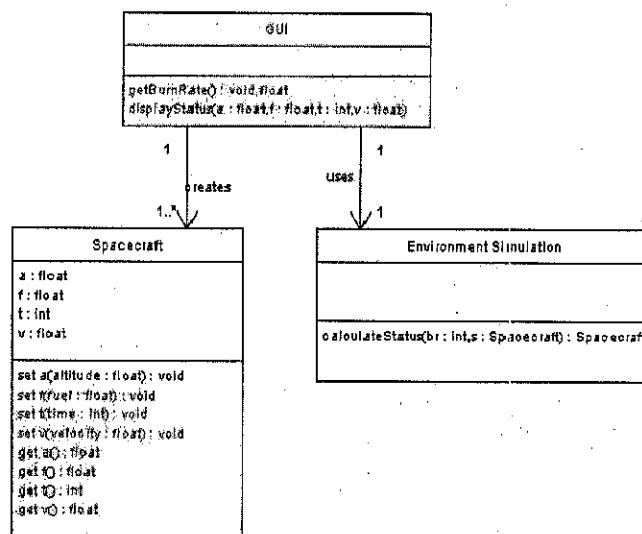


Figure 4-9. UML representation of the classes used in Figure 4-8

**Layered**

Layered styles are as simple and familiar as those above which reflect the traditional use of programming languages like C or Java. The essence of a layered style is that an architecture is separated into ordered layers, wherein a program within one layer may obtain services from a layer below it. The “virtual machines” style is familiar to anyone who has studied computer and operating systems architectures; the client-server layered style is ubiquitous in business applications. Both are discussed below.

#### Virtual Machines

In the virtual machines style a *layer* offers a set of services (“a machine with a bunch of buttons and knobs”) that may be accessed by, at least, programs residing within the layer above it. The services that a layer offers can be termed the “provides interface” of the layer. The services may be implemented by various programs within the layer, but, when designing an architecture, from the perspective of the entities that *use* the layer’s services such distinctions are not apparent. In Figure 4-10 for instance, program A in layer 1 can access the services provided by layer 2; those services may in fact be implemented by programs B and C, but such details are not of concern to program A.

In a strict virtual machines style, programs at a given level may only access the services provided by the layer immediately below it. Thus, again referring to Figure 4-10, program A can only access services provided by layer 2, and not layer 3. A non-strict layered style would allow A to access the services of layer 3 as well.

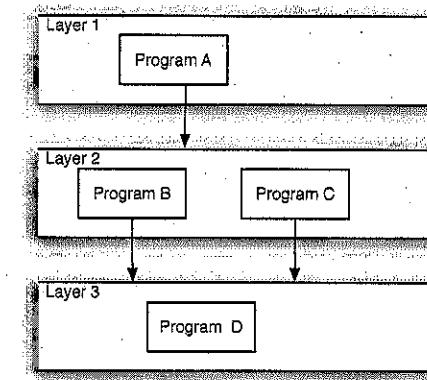


Figure 4-10. Notional layered architecture

Operating systems designs provide the most common use of the layered style. User applications would reside in layer 1, for instance, directory and file manipulation services on level 2, and disk drivers and volume management software at level 3. Networking protocols are also often implemented in a layered style.

#### Style: Virtual Machines

**Summary:** Consists of an ordered sequence of layers; each *layer*, or virtual machine, offers a set of services that may be accessed by programs (sub-components) residing within the layer above it.

**Components:** Layers offering a set of services to other layers, typically comprising several programs (sub-components)

**Connectors:** Typically procedure calls

**Data Elements:** Parameters passed between layers

**Topology:** Linear, for strict virtual machines; a directed acyclic graph in looser interpretations

**Additional constraints imposed:** None.

**Qualities yielded:** Clear dependence structure; software at upper levels immune to changes of implementation within lower levels, as long as the service specifications are invariant. Software at lower levels fully independent of upper levels.

**Rationale:**

**Typical uses:** Operating system design; network protocol stacks.

**Cautions:** Strict virtual machines with many levels can be relatively inefficient.

A four-level version of the lunar lander game is shown in Figure 4-11. The top layer includes all the details of the lunar lander that pertain to the game logic and the environment simulator. The second layer is a generic, 2-D game engine. Such a layer is capable of supporting any of a wide variety of games that only require 2-D graphics. The third layer is the operating system, which provides, among other thing, platform-specific UI support, such as window management and keyboard event management. The bottom layer is provided by firmware or hardware, and provides the physical user interface and computing. Each layer is independent of the layers above it, and only requires access to the services of the layer immediately below it. Note that the focus of this architecture is different than the preceding examples. The explicit inclusion here of a game engine, the operating system, and hardware is intended to help illustrate the layered style.

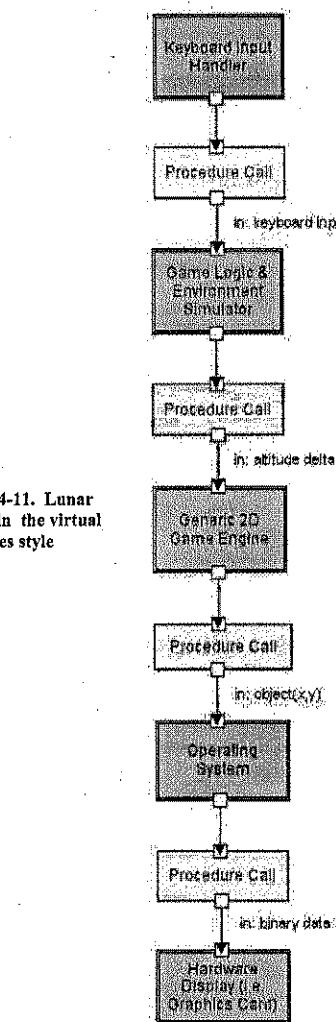


Figure 4-11. Lunar lander in the virtual machines style

*Client-Server*

The client-server style can be simply understood as a two-layer virtual machine with network connections. That is, the server is the virtual machine below the clients, who access the virtual machine's interfaces via remote procedure calls or equivalent network access methods. Typically there are multiple clients who access the same server. The clients are mutually independent; the obligation of the server is to provide the specific services required by each client to that client. Clients are sometimes referred to as "thin" or "thick", reflecting whether they include any significant processing beyond user interface functions.

Grossly simplified, a bank's automated teller machine (ATM) system is a client-server application. The clients are the ATMs; the server is the bank, which keeps track of all accounts and controls all the transactions requested by users at the ATMs.

#### Style: Client-Server

**Summary:** Clients send service requests to the server which performs the required functions and replies as needed with the requested information. The server is aware of clients, but a client is unaware of other clients.

**Components:** Clients and server

**Connectors:** Remote procedure call, network protocols

**Data Elements:** Parameters and return values as sent by the connectors.

**Topology:** Two-level, with multiple clients making requests to the server.

**Additional constraints imposed:** Client to client communication prohibited.

**Qualities yielded:** Centralization of computation and data at the server, with the information made available to remote clients.

#### Rationale:

**Typical uses:** Applications where centralization of data is required, or where processing and data storage benefit from a high-capacity machine, and where clients primarily perform simple user interface tasks, such as many business applications.

**Cautions:** When the network bandwidth is limited and there are a large number of client requests.

A multi-player version of the lunar lander game is shown in Figure 4-12. In the system shown three players simultaneously and independently play the game. All game state, game logic, and environment simulation is performed on the server. The clients perform the user interface functions.

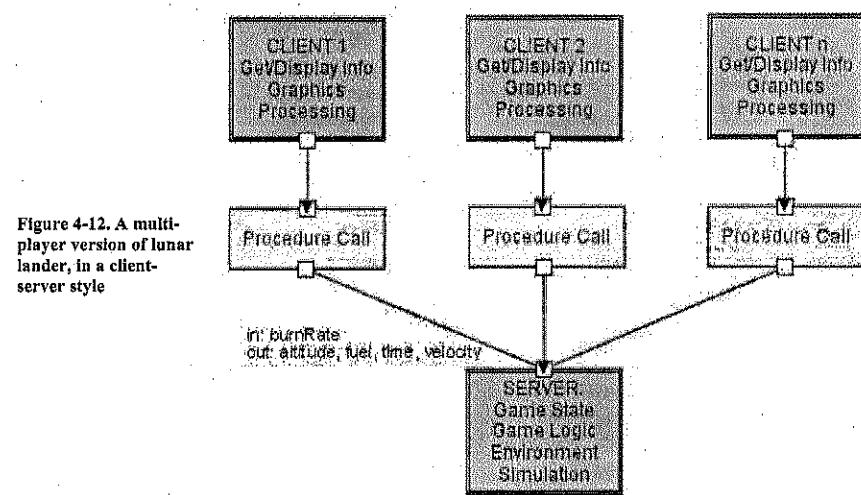


Figure 4-12. A multi-player version of lunar lander, in a client-server style

#### Data-flow Styles

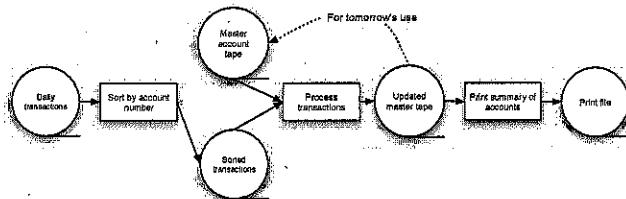
The two styles presented here can be characterized as "data flow" styles. Their essence concerns the movement of data between independent processing elements.

#### Batch Sequential

The batch sequential style is one of the oldest in computer system's design: it arose in the early days of "data processing" when the limitations of computing equipment required that large problems be subdivided into severable components which could communicate by the transfer of magnetic tapes.

A classic example of this style is shown in Figure 4-13. The application is one of updating a bank's record of all its accounts, based upon the processing of the day's transactions (such as a deposit or withdrawal from an account). The process starts with a tape that has all the bank's accounts on it, sorted by account number, and a tape that has the day's transactions on it.

**Figure 4-13. Financial records processed in batch sequential style**



The style is summarized below.

**Style:** Batch Sequential

**Summary:** Separate programs are executed in order; data is passed as an aggregate from one program to the next.

**Components:** Independent programs.

**Connectors:** “The human hand” carrying tapes between the programs, a.k.a. “sneaker-net”<sup>6</sup>

**Data Elements:** Explicit, aggregate elements passed from one component to the next upon completion of the producing program’s execution.

**Topology:** Linear.

**Additional constraints imposed:** One program runs at a time, to completion.

**Qualities yielded:** Severe execution; simplicity

**Rationale:**

**Typical uses:** Transaction processing in financial systems.

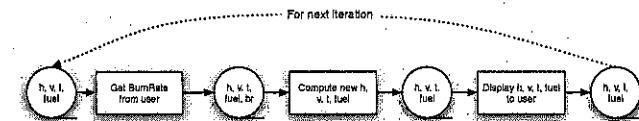
**Cautions:** When interaction between the components is required; when concurrency between components is possible or required.

**Relations to programming languages or environments:** None.

Attempting to build a lunar lander game in the batch sequential style reveals how mismatched the style is to the application. The outline of such a (bizarre) design is presented in Figure 4-14. Here the game state is maintained on magnetic tapes. Each functional processing step of the game is performed by a separate program. Upon performing the step’s function, the program produces an updated version of the game state, which is then handed off to the next program in the process. After the final step of displaying the game state is performed, the produced tape is carried back to the first program for another pass. This is obviously not a highly interactive, real-time game!

<sup>6</sup> Savvy computer operators often wear athletic shoes, more commonly known as “sneakers”.

**Figure 4-14. Lunar Lander: Batch Sequential**



**Pipe and Filter**

Though radically different in detail from Batch Sequential, the pipe-and-filter style introduced in Chapter 1 is also a data flow style. Recall that the essence of the style is that streams of character data are passed from one filter program to another. The filters can operate concurrently, with no requirement for a producing component to finish before a component that consumes the producer’s output begins. Chapter 1 included a natural application of the pipe and filter style to the problem of producing a sorted list of selected file names.

**Style:** Uniform Pipe and Filter

**Summary:** Separate programs are executed, potentially concurrently; data is passed as a stream from one program to the next.

**Components:** Independent programs, known as “filters”.

**Connectors:** Explicit routers of data streams; service provided by operating system.

**Data Elements:** Not explicit; must be (linear) data streams. In the typical Unix/Linux/DOS implementation the streams must be text.

**Topology:** Pipeline, though “T” fittings are possible.

**Qualities yielded:** Filters are mutually independent. Simple structure of incoming and outgoing data streams facilitates novel combinations of filters for new, composed applications.

**Rationale:**

**Typical uses:** Ubiquitous application in operating system’s application programming.

**Cautions:** When complex data structures must be exchanged between filters; when interactivity between the programs is required.

**Relations to programming languages or environments:** Prevalent in Unix shells

A design for the lunar lander game in the pipe and filter style appears in Figure 4-15. Get BurnRate runs looping on its own, always polling the user for a value. When a value is generated it is sent off through the stream connector to the second filter. The second filter runs looping on its

own as well, updating time as it chooses. It serves as the environment simulator and calculates the descent rate of the spacecraft. The third filter likewise loops, updating the display whenever new values become available on its input port. This design follows from a rather functional understanding of the game, similar to the main program and subroutines design.

Figure 4-15. Lunar Lander in pipe-and-filter style



### Shared State

The essence of shared state styles (sometimes colloquially referred to as "shared memory" styles), is that multiple components have access to the same data store, and communicate through that data store. This corresponds roughly to the ill-advised practice of using global data in C or Pascal programming. The difference is that with shared state styles the center of design attention is on these structured, shared repositories, and that consequently they are well-ordered and carefully managed. The use of global data in programming is usually only one of several means of communication between subprograms, and is done as an expedience.

### Blackboard

The blackboard style arose in artificial intelligence applications. The intuitive sense of the style is one of many diverse experts sitting around a blackboard, all attempting to cooperate in the solution of a large, complex problem. As any given expert recognizes some part of the problem on the blackboard for which he feels competent to solve, he grabs that subproblem, goes away and works on it, and when finished posts the solution back on the blackboard. Posting of that solution may enable another expert to identify a problem which he can solve, and so the process continues until the whole problem is solved. Thus the state of information on the blackboard determines the order of execution of the various "expert" programs.

#### Style: Blackboard

**Summary:** Independent programs access and communicate exclusively through a global data repository (a.k.a. blackboard).

**Components:** Independent programs (sometimes referred to as "knowledge sources"), blackboard

**Connectors:** Access to the blackboard may be by direct memory reference, or can be through a procedure call or a database query.

**Data Elements:** Data stored in the blackboard

**Topology:** Star topology, with the blackboard at the center.

**Variants:** In one version of the style programs poll the blackboard to determine if any values of interest have changed; in another version a blackboard manager notifies interested components of an update to the blackboard.

**Qualities yielded:** Complete solution strategies to complex problems do not have to be pre-planned. Evolving views of the data/problem determine the strategies that are adopted.

### Rationale:

**Typical uses:** Heuristic problem solving in artificial intelligence applications.

**Cautions:** When a well-structured solution strategy is available; when interactions between the independent programs require complex regulation; when representation of the data on the blackboard is subject to frequent change (requiring propagating changes to all the participating components).

**Relations to programming languages or environments:** Versions of the blackboard style which allow concurrency between the constituent programs require concurrency primitives for managing the shared blackboard.

Figure shows the lunar lander program solved in a blackboard style. Here, a single connector regulates access from the various "experts" in manipulating the information on the blackboard. The blackboard maintains the game state; the experts perform the independent tasks of (1) updating the descent engine burn rate based upon input from the user, (2) displaying to the user the current state of the spacecraft and any other aspect of the game state, and (3) updating the game state based upon a time and physics model. That is, the third component determines how fast time passes and updates the game state in accordance with the passage of time and the physics model of the moon and the lander.

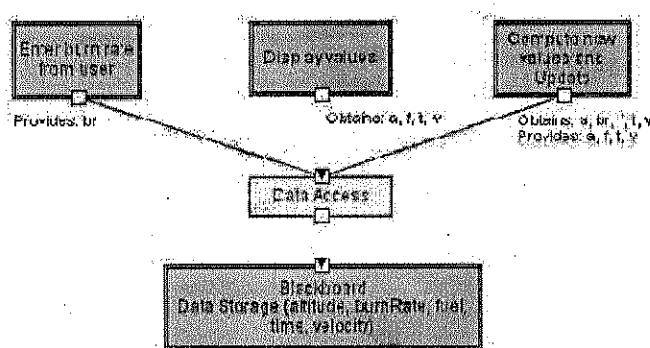


Figure 4-16. Lunar lander in the blackboard style

#### Rule-Based/Expert System

A rule-based architecture is a highly specialized type of shared memory architecture. The shared memory is a so-called knowledge base, i.e. a database which contains facts (statements of values of variables) and production rules which consist of “if...then” clauses over the set of variables. A user interface component provides two modes: one for entering facts and production rules and another for entering queries, known as goals. Operating on the knowledge base, in response to user input, is an inference engine. Facts and production rules are added to the knowledge base; goals are compared against existing facts in the database. If an exact match is found, it returns *true* to the user interface. Otherwise, it evaluates the rules as necessary to determine the validity of the goal.

##### Style: Rule-based/expert system

**Summary:** Inference engine parses user input and determines whether it is a fact/rule or a query. If it is a fact/rule, it adds this entry to the knowledge base. Otherwise, it queries the knowledge base for applicable rules and attempts to resolve the query.

**Components:** User interface, inference engine, knowledge base

**Connectors:** Components are tightly interconnected, with direct procedure calls and/or shared memory.

**Data Elements:** Facts and queries

**Topology:** Tightly coupled three-tier (direct connection of user interface, inference engine, and knowledge base)

**Qualities yielded:** Behavior of the application can be very easily modified through addition or deletion of rules from the knowledge base. Small systems can be quickly prototyped. Thus useful for iteratively exploring problems whose general solution approach is unclear.

#### Rationale:

**Typical uses:** When the problem can be understood as matter of repeatedly resolving a set of predicates.

**Cautions:** When a large number of rules are involved understanding the interactions between multiple rules affected by the same facts can become very difficult. Understanding the logical basis for a computed result can be as important as the result itself.

**Relations to programming languages or environments:** Prolog is a common language for building rule-based systems.

Designing a solution for the lunar lander problem in the rule-based style requires thinking of the problem as one of maintaining a set of consistent facts about the spacecraft. This is pretty “natural”, as the physics model that determines the state of the spacecraft can be so understood. For instance, the passage of 1 second of time demands that the facts of the amount of fuel remaining, the velocity of the spacecraft, and the height of the spacecraft be brought up to date, consistently.

With regard to the user interaction model, in the example solution shown in Figure 4-17, the user enters the value of burn rate as a fact:

`burnrate(25)`

To see what the status of the spacecraft is, the user can switch to the goal mode and asks whether the spacecraft has landed safely

`landed(spacecraft)`

To handle this query, the inference engine queries the database. If the existing facts and other production rules satisfy the conditions “height <= 0” and “velocity < 3 ft/s<sup>2</sup>”, then the engine returns true to the user interface. Otherwise, it returns false<sup>7</sup>.

<sup>7</sup> For a realistic model, the set of rules in the database will be extensive to perform the computation of a, v, t, f. A simple one dimensional physics equation calculates altitude as follows:  $\frac{1}{2} * (\text{accelerationThrust} - \text{accelerationGravity}) * t^2 + v * t + \text{altitudeOld}$ . However, a more realistic calculation of thrust is quite complicated (see notes at the end of the chapter for references).

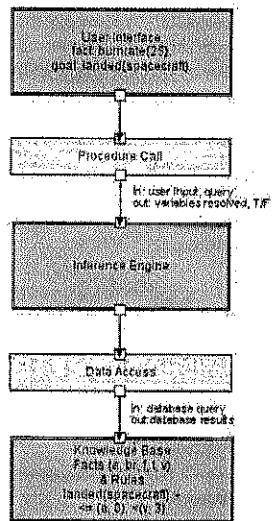


Figure 4-17. Lunar lander in an rule-based style

### Interpreter

The distinctive characteristic of interpreter styles is dynamic, “on-the-fly” interpretation of commands. Commands are explicit statements, possibly created moments before they are executed, possibly encoded in human-readable and editable text. Commands are phrased in terms of pre-defined primitive commands. Interpretation proceeds by starting with an initial execution state, obtaining the first command to execute (possibly by reading some user input), executing the command over the current execution state, thereby modifying that state, then proceeding to execute the next command. Identification of the “next command” may be affected by the result of executing the previous command; indeed, in the general case the next command may be the product of the execution of the previous command.

The *basic interpreter* architectural style involves the execution of commands one at a time. Similarly, though typically at a larger granularity, the *mobile code* style involves the execution of one chunk of code at a time. The difference with mobile code is that the place where the commands are executed may vary over time.

#### Basic Interpreter

Execution of commands in the basic interpreter style is similar to the rule-based style described above, where the inference engine parses a command input and performs variable resolution based on the knowledge repository. In the case of the basic interpreter style the command interpreter is more general (capable of more generic operations than performing inferences over a set of rules). The interpretation of a single command may involve numerous primitive operations. The knowledge repository is similarly more general since arbitrary data structures may be involved.

While perhaps sounding complicated, the interpreter style is quite familiar to what might be the world’s largest cohort of programmers: the users of Microsoft Excel. Excel’s formulas are in fact commands interpreted by the Excel execution engine – the interpreter. Similarly Excel’s macros are interpreted by the Visual Basic interpreter. Many graphical editing programs are similarly interpreter based: a structure of “text” commands describing the drawing is maintained by the drawing program. The drawing on the screen seen by the user is created by an internal interpreter running over the text, interpreting it, issuing drawing commands to the graphics engine.

#### Style: Interpreter

**Summary:** Interpreter parses and executes input commands, updating the state maintained by the interpreter

**Components:** Command interpreter, program/interpreter state, user interface.

**Connectors:** Typically the command interpreter, user interface, and state are very closely bound with direct procedure calls and shared state.

**Data Elements:** Commands.

**Topology:** Tightly coupled three-tier; state can be separated from the interpreter.

**Qualities yielded** Highly dynamic behavior possible, where the set of commands is dynamically modified. System architecture may remain constant while new capabilities are created based upon existing primitives.

#### Rationale:

**Typical uses:** Superb for end-user programmability; supports dynamically changing set of capabilities

**Cautions:** When fast processing is needed (it takes longer to execute interpreted code than executable code); memory management may be an issue, especially when multiple interpreters are invoked simultaneously.

**Relations to programming languages or environments:** Lisp and Scheme are interpretive languages, and sometimes used when building other interpreters.

In the version of the Lunar Lander game shown in Figure 4-18, for each command entered, the interpreter engine parses the code and updates the interpreter state when necessary. The commands in this case are specific directives regarding how the spacecraft should be manipulated – most importantly, how the descent engine should be throttled. The interpreter, thus, has been programmed specifically to interpret such commands. It then displays back to the user the result of execution. Thus, when the user enters (*burn, 50*), the interpreter takes the first parameter as the command and the second command as the amount of fuel to burn. This then is parsed by the interpreter and makes the necessary updates to the altitude, fuel level, and velocity. Time is simulated by having *t* incremented by 1 each time the user enters a burn command. When the user enters the check status command, the user receives the current state of altitude, fuel, time, and velocity..

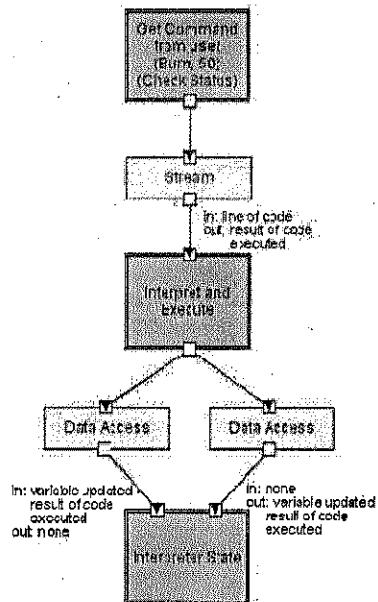


Figure 4-18. Lunar lander in an Interpreter style

#### Mobile Code

As the name suggests, mobile code styles enable code to be transmitted to a remote host for interpretation. This may be due to a lack of local computing power, lack of resources, or due to large data sets located remotely. Mobile code may be classified as code on demand, remote

evaluation, or mobile agent depending on where the code is being transmitted, who requested the transmission, and where the program state resides. Code on demand is when the “initiator” has resources and state but downloads code from another site to be executed locally. Remote evaluation is when the “initiator” has the code but lacks the resources (such as the interpreter) to execute the code. Thus, it transmits code to be processed at a remote host, such as in grid computing. Results are returned to the initiator. Mobile agent is when the “initiator” has the code and the state but some of resources are located elsewhere. Thus the “initiator” moves to a remote host with the code, the state, and some of the resources. Processing need not return to the initiator.

In all of the mobile code styles, a data element (some representation of a program) is dynamically transformed into a data processing component (when those commands are interpreted or otherwise executed).

#### Style: Mobile Code

**Summary:** Code, and according to the variant, state, moves to be interpreted on another host

**Components:** “Execution dock”, which handles receipt and deployment of code and state; code compiler/interpreter

**Connectors:** Network protocols and elements for packaging code and data for transmission.

**Data Elements:** Representations of code as data; program state; data

**Topology:** Network

**Variants:** Code-on-demand, remote evaluation, and mobile agent.

**Qualities yielded:** Dynamic adaptability. Takes advantage of the aggregate computing power of available hosts; increased dependability through provision of migration to new hosts.

#### Rationale:

**Typical uses:** When processing large data sets in distributed locations, it becomes more efficient to have the code move to the location of these large data sets; when it is desirable to dynamically customize a local processing node through inclusion of external code.

**Cautions:** Security issues: execution of imported code may expose the host machine to malware. Other cautions: when it is necessary to tightly control the different software versions deployed; when costs of transmission exceed the cost of computation; when network connections are unreliable.

**Relations to programming languages or environments:** Scripting languages (i.e. JavaScript, VBScript), ActiveX control, embedded Word/Excel macros. Grid computing

In Figure 4-19, client web browsers download code-on-demand Lunar Lander Game Applet via HTTP. Thus, all the game logic moves to the

client machine, freeing the server's computing resources. In the figure as shown, each client machine maintains the game state independently of other clients. The "execution dock" components are not shown. Should state be maintained by the server a more interesting configuration results.

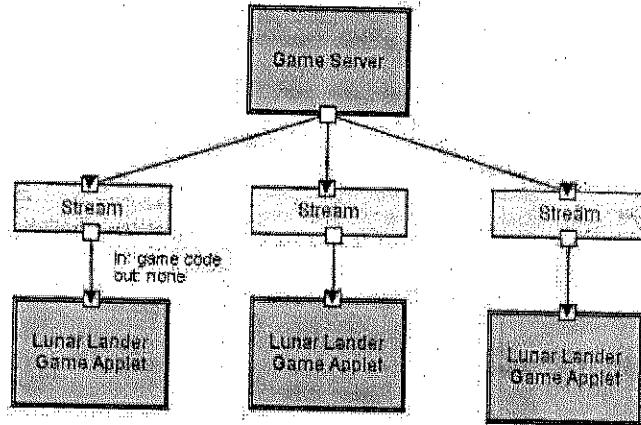


Figure 4-19. Lunar lander as code-on-demand

#### Implicit Invocation

Unlike the previous styles discussed, the two styles discussed below are characterized by calls that are invoked indirectly and implicitly as a response to a notification or an event. Enhanced scalability is one of the benefits of the indirect interaction between loosely-coupled components.

#### Publish-Subscribe

Publish-subscribe takes its name from the analogous relationship between magazine or newspaper publishers and their subscribers. The publisher periodically creates information and the subscriber obtains a copy of the information or at least is informed of its availability. The architectural style reflects this kind of relationship. Several variants exist, differing in the distance between the publisher and the subscribers, and the way in which the relationship is managed.

In a simple pub-sub style the publisher maintains a list of subscribers to each of which a procedure call is issued when new information is available. Subscribers register their interest with publishers, providing them with the procedure interface to be used (the "call back") when

information is published. Subscribers can also de-register their interest, having the call-back removed from the subscriber's subscription list.

The simple pub-sub style works well within the context of a simple program. For large-scale, network-based applications a more sophisticated set of services is needed. Publishers need to "advertise" the existence of information resources to which others may subscribe, either at system start-up, periodically, or on demand. Subscriptions can no longer take the form of call-back procedure, but involve the use of network protocols. Efficiency concerns argue against point-to-point relationships between publishers and subscribers; intermediate proxies or caches can help performance – just as with physical newspapers, where a paperboy serves as proxy for the newspaper company, being responsible for delivery of the papers within a small geographic region.

The publish-subscribe style caters to applications where there is a clear delineation between producers and consumers of information. A familiar network-based application of the publish-subscribe style is an online job posting service. Hiring managers post, or publish, the job openings. Meanwhile, job seekers subscribe to the online service to receive notifications of new job postings. While this application works with perhaps only a few notifications per day, other network pub-sub applications operate with many notifications per second.

#### Style: Publish-Subscribe

**Summary:** Subscribers register/deregister to receive specific messages or specific content. Publishers broadcast messages to subscribers either synchronously or asynchronously.

**Components:** Publishers, subscribers, proxies for managing distribution

**Connectors:** Procedure calls may be used within programs, more typically a network protocol is required. Content-based subscription requires sophisticated connectors.

**Data Elements:** Subscriptions, notifications, published information

**Topology:** Subscribers connect to publishers either directly or may receive notifications via a network protocol from intermediaries

**Variants:** Specific uses of the style may require particular steps for subscribing and unsubscribing. Support for complex matching of subscription interests and available information may be provided and be performed by intermediaries.

**Qualities yielded** Highly efficient one-way dissemination of information with very low-coupling of components

#### Rationale:

**Typical uses:** News dissemination: whether in the real world or on-line events. Graphical user interface programming. Multi-player network based games.

**Cautions:** When the number of subscribers for a single data item is very large a more specialized broadcast protocol will likely be superior.  
**Relations to programming languages or environments:** In large-scale systems support for pub-sub provided by commercial “middleware” technology.

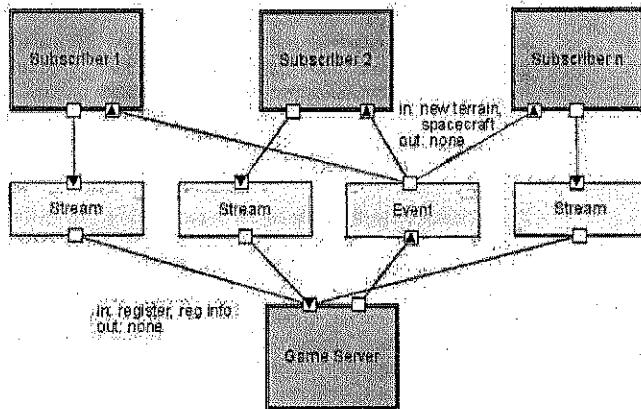


Figure 4-20. Lunar lander in Pub-Sub

In the example of Figure 4-20, the Lunar Lander game is deployed to various network hosts. Players register their hosts to a game server which publishes information, such as new lunar terrain data, new spacecraft, and the location of the registered spacecraft. Once registered, the subscribed hosts receive notifications when any of the information that have registered for has been updated. Players may elect to download the new data to their local Lunar Lander game.

#### Event-based

The event-based style is characterized by independent components communicating solely by sending events through event-bus connectors. In its “purest” form, components emit events to the event-bus which then transmits them to every other component. Components may react in response to receipt of an event or may ignore it; the architectural style does not make any specific demand. While seeming to perhaps be rather chaotic and unpredictable, this style is roughly analogous as to how we, as humans, behave in society. We are continually receiving – through our senses – events from the outside world: some we react to and some we ignore. Similarly we are continually emitting events into the world, such as by speaking. Again, sometimes they elicit a response from others and sometimes not. Such as when you are talking to your teen-age son.

For efficiency reasons the pure form of event-based architectures is seldom used; it is more efficient to only distribute events to those components who express an interest in them. With this optimization the style becomes similar to publish-subscribe. The distinctive character of the event-based style, however, is that there is no classification of components into “publishers” and “subscribers”; all components potentially both emit and receive events. With the event-based style the optimization of event distribution is the responsibility of the connectors; registration of interest in particular events is only handled by the connectors. Similarly replication of events for delivery to multiple recipients may take place late in the transmission process and would be transparent to both the event emitter and the event receiver. Finally event distribution may be handled either on a push- or pull- basis. In the case of “pull”, or polling, event recipients can query the connector to see if a new event is available. Such a query could either be blocking (the component waits until an event is available) or non-blocking (the component returns immediately, either with a new value – if available – or not).

The event-based style is highly suited to strongly decoupled concurrent components, where at any given moment a component may either be creating information of potential interest to others, or consuming information. A classic example usage is in financial markets: independent companies (traders) may want to know the latest price of a commodity being sold in London; similarly when that trader completes a deal, the results of that trade represent information of interest to others around the world.

#### Style: Event-based

**Summary:** Independent components asynchronously emit and receive events communicated over event buses

**Components:** Independent, concurrent event generators and/or consumers

**Connectors:** Event buses (at least one)

**Data Elements:** Events – data sent as a first-class entity over the event bus

**Topology:** Components communicate with the event buses, not directly to each other. More than one event bus may be used; event buses may directly transmit events.

**Variants:** Component communication with the event bus may either be push or pull based.

**Qualities yielded:** Highly scalable, easy to evolve, effective for highly distributed applications.

#### Rationale:

**Typical uses:** user interface software, wide-area applications involving independent parties (e.g. financial markets)

**Cautions:** No guarantee if or when an particular event will be processed.  
**Relations to programming languages or environments:** Commercial message-oriented middleware technologies support event-based architectures.

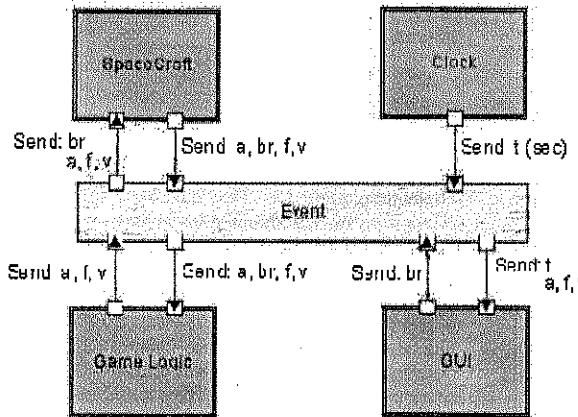


Figure 4-21. Lunar lander in the event-based style.

Figure 4-21 shows the lunar lander designed in an event-based style. The clock component drives the game. Every fraction of a second, the clock component sends out a ‘tick’ notification on the event bus. Upon receiving a pre-defined number of notifications, the graphical user-interface prompts the user for the burn rate. When obtained, a notification of the new burn rate is sent on the event bus. Upon receipt of this notification the SpaceCraft component updates its model of the spacecraft. The SpaceCraft component, also upon receiving a pre-defined number of notifications from the clock, recalculates the spacecraft altitude, fuel level, and velocity, and then emits those values to the event bus. The GameLogic component, receiving both information about the state of the spacecraft and the amount of time that has passed, determines whether the game is over, and if so what the final condition of the spacecraft was when the game ended. A notification that the values have been updated prompts the user interface to display this information to the user.

#### “Implicit Invocation”

“Implicit Invocation” describes the execution model of both publish-subscribe and event-based styles. An action, such as invocation of a procedure, may be taken as the result of some activity occurring elsewhere

in the system, but the two activities are distant from one another. The invocation is indirect, since there is no direct coupling between the components involved. The invocation is implicit, since the causing component has no awareness that its action ultimately causes an invocation elsewhere in the system.

#### Peer-to-Peer

The peer-to-peer (p2p) architectural style consists of a network of loosely-coupled autonomous peers, each peer acting both as a client and a server. Peers communicate using a network protocol, sometimes specialized for p2p communication – such was the case for the original Napster and Gnutella file sharing applications. Unlike the Client-Server style where state and logic are centralized on the server, p2p decentralizes both information and control. Absence of centralization makes resource discovery an important issue for p2p applications. In a pure p2p application queries for information are issued to the network of peers at large; requests propagate until the information is discovered or some threshold is passed. If the desired information is located the peer obtains the direct address of that peer and contacts it directly. This style is limited by the network algorithm used to query the system and the network bandwidth available. Hybrid applications optimize this process by having certain peers play ‘special roles’, either for locating other peers or for providing directories locating information. The original Napster, for example, was not a true peer-to-peer application because it used a centralized server for indexing music and locating other peers. Although the term “peer-to-peer” has been popularized by file-sharing applications, it enables a host of applications such as business-to-business commerce, chat, remote collaboration, and sensor networks.

#### Style: Peer-to-peer

**Summary:** State and behavior are distributed among peers which can act as either clients or servers.

**Components:** Peers: independent components, having their own state and control thread.

**Connectors:** Network protocols, often custom.

**Data Elements:** Network messages

**Topology:** Network (may have redundant connections between peers); can vary arbitrarily and dynamically

**Qualities yielded:** Decentralized computing with flow of control and resources distributed among peers. Highly robust in the face of failure of any given node. Scalable in terms of access to resources and computing power

#### Rationale:

**Typical uses:** Where sources of information and operations are distributed and network is ad-hoc

**Cautions:** When information retrieval is time critical and cannot afford the latency imposed by the protocol. P2p networks must make provision for malicious peers and managing trust in an open environment.

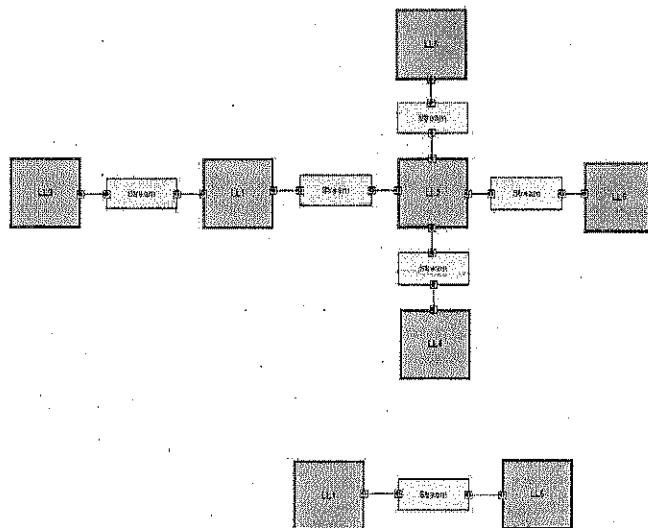


Figure 4-22. Lunar lander as a P2p application

In the example of Figure 4-22, a group of Lunar Lander spacecraft are on their way to land in different parts of the moon. Multiple landers are used in this example to highlight that the p2p architectural style is designed to support interaction between highly autonomous components, and especially application contexts where the number of participating components may vary over time. Lunar Lander 1 (LL1) wants to find out if another spacecraft has already landed in a specific location, so that collisions can be avoided. Each of the spacecraft is configured to communicate with the others using a p2p protocol over a network. A spacecraft will only be able to communicate with others that are within a specified distance.

Lunar Lander 1 will go through the following steps to obtain the information:

1. LL1 queries for available spacecraft, i.e. spacecraft within communication range.
2. LL2 and LL3 respond.

3. LL1 queries if LL2 and LL3 have the requisite information
4. LL2 passes on the query to its adjacent nodes, LL4, LL5, and LL6.
5. LL5 responds to LL1 that it has the desired information, and passes the information along.
6. LL2 passes the response back to LL1
7. Alternatively, if LL5 comes within range, LL1 subsequently directly contacts LL5 and queries it for the information – shown at the bottom of the figure.

#### 4.3.5 More Complex Styles

The C2 and distributed objects styles combine elements of several of the preceding styles to yield powerful design tools capable of handling challenging problems. They have both resulted from an extended period of engineering experimentation, in which numerous design trade-offs were made.

The C2 (“Components and Connectors”) style grew out of a desire to obtain the benefits of the model-view-controller pattern in a distributed, heterogeneous platform setting. Concepts from layered and event-based architectures were added. The resulting style, though originally developed to support graphical user interface applications, was found to be beneficial in a wide variety of applications – indeed more so outside the domain of GUIs than within. Its primary interest in this text is in showing how elements of many styles may be judiciously combined to meet a variety of needs.

The distributed objects style has its roots in the object-oriented style. As with C2, its developers sought to extend the benefits of this core style to a distributed heterogeneous world. Interoperability between components or objects implemented in different programming languages is achieved via the use of connectors and adapters. The most obvious difference between the two styles is that several networking concerns are explicitly addressed in the distributed objects style.

#### C2

C2 is a much more complicated style than those considered above, so to motivate the complexity we start by listing some of the benefits sought and achieved through application of the style:

- Substrate independence: ease in moving the application to work utilizing new “platforms”, such as operating systems and user interface toolkits;
- Heterogeneous applications: enabling an application to be comprised of components written in more than one programming language and running on multiple, varying hardware platforms, communicating across a network;

- Support for product lines: ease of substituting one component for another to achieve similar but different applications;
- Ability to design in the model-view-controller style, but with very strong separation between the model and the user interface elements;
- Support for concurrent components;
- Support for network-distributed applications.

Each of these benefits has been seen in the simple styles above; the contribution of C2 is combining selected simple styles into a coherent comprehensive approach. The following paragraphs lay out C2's constraints.

[Topology] C2 can be summarized as a network of concurrent components hooked together by message routing connectors. C2 depends entirely upon implicit invocation. All components and connectors have a defined top and bottom. The top of a component may be connected to the bottom of a single connector and the bottom of a component may be connected to the top of a single connector. No direct component-to-component links are allowed; there is, however, no bound on the number of components or connectors that may be attached to a single connector. When two connectors are attached to each other, it must be from the bottom of one to the top of the other. These rules induce layering which promotes substrate independence and component substitutability.

[Message-based communication] All communication between components is achieved by exchanging messages. Messages are classified as either requests (a specific asking for a service to be performed) or notifications (statements of facts about the system, such as the change in value of some object). This requirement is suggested by the asynchronous nature of applications wherein users and the application perform actions concurrently and at arbitrary times, and where various components in the architecture must be notified of those actions.

[Message flow and Substrate Independence] Requests flow upwards in an architecture; notifications flow downwards. Central to the style is a principle of limited visibility or "substrate independence": a component within the hierarchy can only be aware of components 'above' it and is completely unaware of components which reside 'beneath' it. Since downwards communication is limited to the emitting of notifications, a component cannot know which components below it (if any) will react to receipt of a notification.

[Interfaces] Each component has a top and bottom domain. The top domain specifies the set of notifications to which a component may react, and the set of requests that the component emits up an architecture. The

bottom domain specifies the set of notifications that this component emits down an architecture, and the set of requests to which it responds.

Notions of above and below are used to support an intuitive understanding of the architectural style. As is typical with virtual machine diagrams found in operating systems textbooks, the application code is (arbitrarily) regarded as being at the top, while user interface toolkits, windowing systems, and physical devices (including those that humans interact with) are at the bottom. Substrate independence has a clear potential for fostering substitutability and reusability of components across architectures.

One issue that must be addressed, however, is the apparent dependence of a given component on its 'superstrate', i.e. the components above it, since a component can issue a specific request upwards in an architecture. If each component is built so that its top domain closely corresponds to the bottom domains of those components with which it is specifically intended to interact in the given architecture, its reusability value is greatly diminished, and it can only be substituted by components with similarly constrained top domains. For that reason, C2 introduces the notion of event translation. Domain translation is a transformation of the requests issued by a component into the specific form understood by the recipient of the request, as well as the transformation of notifications received by a component into a form it understands.

C2 also supports compositionality, or hierarchical composition, where an entire architecture becomes a single component in another, larger architecture. Each component may have its own thread(s) of control. It simplifies modeling and programming of multi-component, multi-user and concurrent applications, and enables exploitation of distributed platforms. Finally, there is no assumption of a shared address space among components. Any premise of a shared address space would be unreasonable in an architectural style that allows composition of heterogeneous, highly distributed components, developed in different languages, with their own threads of control, internal structures and domains of discourse.

A simple C2 architecture for the lunar lander application is shown in Figure 4-23. It operates much like the solution shown in Figure 4-21, the event-based style.

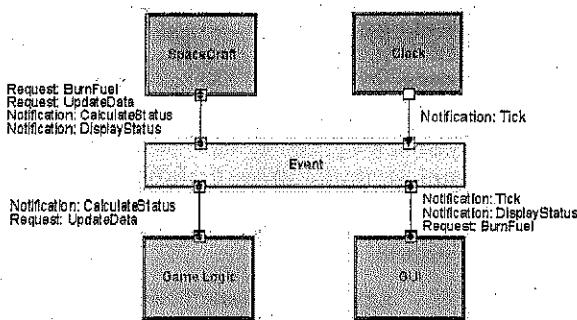


Figure 4-23. Lunar Lander in the C2 style

#### Style: C2

**Summary:** An indirect invocation style in which independent components communicate exclusively through message routing connectors. Strict rules on connections between components and connectors induce layering.

**Components:** Independent, potentially concurrent message generators and/or consumers

**Connectors:** Message routers that may filter, translate, and broadcast messages of two kinds: notifications and requests.

**Data Elements:** Messages – data sent as first-class entities over the connectors. Notification messages announce changes of state. Request messages request performance of an action.

**Topology:** Layers of components and connectors, with a defined “top” and “bottom”, wherein notifications flow downwards and requests upwards.

#### Additional constraints imposed:

- All components and connectors have a defined top and bottom. The top of a component may be attached to the bottom of a single connector and the bottom of a component may be attached to the top of a single connector. No direct component-to-component links are allowed; there is, however, no bound on the number of components or connectors that may be attached to a single connector. When two connectors are attached to each other, it must be from the bottom of one to the top of the other.
- Each component has a top and bottom *domain*. The top domain specifies the set of notifications to which a component may react and the set of requests that the component emits up an architecture. The bottom domain specifies the set of notifications that this component emits down an architecture and the set of requests to which it responds.

- Components may be hierarchically composed, where an entire architecture becomes a single component in another, larger architecture.
- Each component may have its own thread(s) of control.
- There can be no assumption of a shared address space among components.

#### Qualities yielded:

- Substrate independence: ease in moving the application to new platforms (including operating system and user interface toolkit);
- Heterogeneous applications: components can be built in different programming languages and run on different hardware platforms;
- Support for product lines: ease of substituting one component for another to achieve related but different applications;
- Ability to program in the model-view-controller style, but with very strong separation between the model and the user interface elements;
- Support for concurrent components;
- Support for network-distributed applications.

#### Rationale:

**Typical uses:** Reactive, heterogeneous applications. Applications demanding low-cost adaptability.

**Cautions:** Event-routing across multiple layers can be inefficient. Overhead high for some simple kinds of component interaction.

**Relations to programming languages or environments:** Programming frameworks are used to facilitate creation of implementations faithful to architectures in the style. Support for Java, C, Ada.

A more instructive application of C2 is shown in Figure 4-25, in which a KLAX-like game is supported. A screenshot from the game is shown in Figure 4-24. The essence of the game is that colored tiles fall from the chutes at the top of the user’s screen. A “palette” is used to move horizontally across the screen; it can catch the tiles as they fall from the chutes. By inverting the palette the tiles can be dropped into the wells below. By matching three or more tiles of the same color, horizontally, vertically, or diagonally across the wells, points are scored and the tiles subsequently removed from the game board. If tiles are not caught by the palette lives are “lost”; similarly if the wells are allowed to overflow.

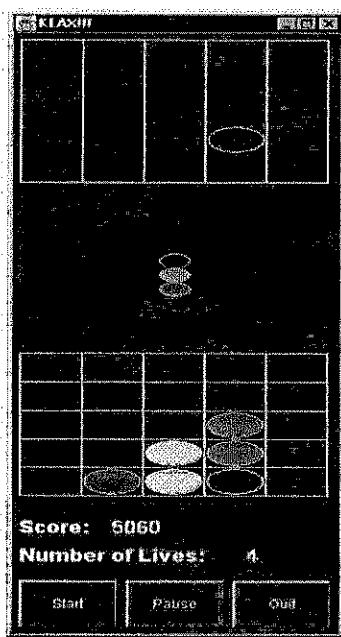


Figure 4-24.  
Screenshot of example  
KLAX-like game

The components that make up the KLAX-like game can be divided into three logical groups. At the top of the architecture are the components which encapsulate the game's state plus the clock. These components are placed at the top since the game state is vital for the functioning of the other two groups of components. The game state components receive no notifications, but respond to requests and emit notifications of internal state changes. In a sense these components play the role of servers, or perhaps of blackboards. Notifications are directed to the next level, where they are received by both the game logic components and the artist components.

The game logic components request changes of game state in accordance with game rules, and interpret game state change notifications to determine the state of the game in progress. For example, if a tile is dropped from the well, RelativePositioningLogic determines if the palette is in a position to catch the tile. If so, a request is sent to PaletteADT to catch the tile. Otherwise, a notification is sent that a tile has been dropped. This notification is detected by StatusLogic, causing the number of lives to

be decremented. The logic components perform their functions in response to receipt of a particular number of notifications from the clock.

The artist components receive notifications of game-state changes, causing them to update their depictions. Each artist maintains the state of a set of abstract graphical objects which, when modified, send state change notifications in the hope that a lower-level graphics component will render them on the screen. TileArtist provides a flexible presentation for tiles. Artists maintain information about the placement of abstract tile objects. TileArtist intercepts any notifications about tile objects and recasts them to notifications about more concrete drawable objects. For example, a 'Tile-Created' notification might be translated into a 'Rectangle-Created' notification. The LayoutManager component receives all notifications from the artists and offsets any coordinates to ensure that the game elements are drawn in the correct two-dimensional juxtaposition. The GraphicsBinding component receives all notifications about the state of the artists' graphical objects and translates them into calls to a window system. User events, such as a key press, are translated into requests to the artist components.

The application of the C2 style to this problem yields several benefits. One is the easy creation of related, but different, games. By substitution of three components the game can be transformed into one where letters fall down the chutes instead of tiles, and the game logic is based upon spelling words in the wells. The components involved are the tile artist, tile match logic, and next tile placing logic, which become the letter artist, word match logic, and next letter placing logic components, respectively. Similarly confined and easy substitutions or additions of components result in network-based multi-player games, a high-score version, and so on. The application can run over network boundaries, the user interface toolkit can be swapped out without modification to the various artists, and components can execute concurrently.

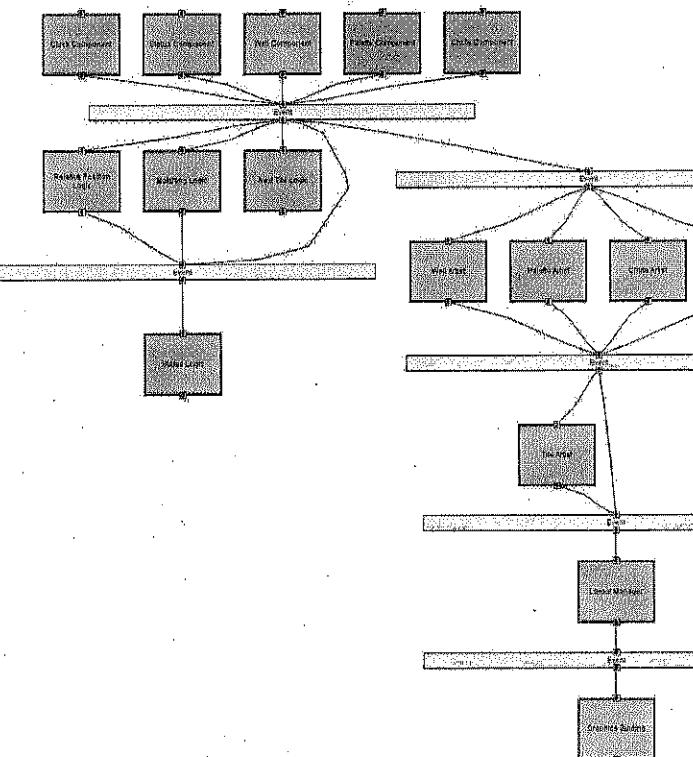


Figure 4-25. A KLAX-like video game in the C2 style

### Distributed Objects

This distributed objects style represents a combination and adaptation of several simpler styles. The fundamental vocabulary comes, of course, from the simple object-oriented style considered earlier in this chapter. This style is augmented with the client-server style to provide the notion of distributed objects, with access to those objects from, potentially, different processes executing on different computers. The posited need for cross-machine and cross-language communication puts a constraint on the communication between the processes, however, and hence to some extent the influence of pipe-and-filter is seen, with serialization of parameters (data marshalling) for communication.

In this style, therefore, objects, in the standard object-oriented terminology sense, are instantiated on different hosts, each of which exposes a public interface. The “objects” can be anything from data structures to million-line legacy systems. The interfaces are special in that all the parameters and return values must be serializable so they can go over the network. The default mode of interaction between objects is synchronous procedure call, although asynchronous extensions are found in some particular versions of distributed objects, such as CORBA.

#### Style: Distributed Objects

**Summary:** Application functionality broken up into “objects” (coarse- or fine-grained) that can run on heterogeneous hosts and can be written in heterogeneous programming languages. Objects provide services to other objects through well-defined provided interfaces. Objects invoke methods across host, process, and language boundaries via remote procedure calls (RPCs), generally facilitated by middleware.

**Components:** Objects (software components exposing services through well-defined provided interfaces)

**Connector:** (Remote) Method invocation

**Data Elements:** Arguments to methods, return values, and exceptions

**Topology:** General graph of objects from callers to callees; in general required services are not explicitly represented.

**Additional constraints imposed:** Data passed in remote procedure calls must be serializable. Callers must deal with exceptions that can arise due to network or process faults.

**Qualities yielded:** Strict separation of interfaces from implementations as well as other qualities of object-oriented systems in general, plus mostly-transparent interoperability across location, platform, and language boundaries.

#### Rationale:

**Typical uses:** Creation of distributed software systems composed of components running on different hosts. Integration of software components written in different programming languages or for different platforms.

**Cautions:** Interactions tend to be mostly synchronous and do not take advantage of the concurrency present in distributed systems. Users wanting services provided by the middleware (network, location, language transparency) often find that the middleware induces the distributed objects style on their applications whether or not it is the best style. Difficulty dealing with streams and high-volume data flows.

#### Relations to programming languages or environments:

Implementations in almost every programming language and environment.

#### CORBA

CORBA is a standard for implementing middleware that supports development of applications composed of distributed objects. Many software development practitioners will have experience with, or at least heard of, CORBA technology. However, CORBA's relationship to software architecture and architectural styles is not always clear. This section will describe CORBA and its architectural implications.

The basic idea behind CORBA is that an application is broken up into "objects," which are effectively software components that expose one or more provided interfaces. In CORBA, these provided interfaces are specified in terms of a programming-language-and platform-neutral notation called the Interface Definition Language (IDL). IDL closely resembles the way class interfaces are specified in an object-oriented programming language. An IDL description of the interface for the data store component of a Lunar Lander system might look like this:

```
interface IDataStore{
    int getAltitude();
    void setAltitude(in int newAltitude);

    int getBurnRate();
    void setBurnRate(in int newBurnRate);

    void getStatus(out int altitude, out int burnRate,
                  out int velocity, out int fuel,
                  out int time);
}
```

All access to an object occurs through calls to one of its IDL-specified interfaces. IDL is strongly-typed, meaning that calls and parameters can be type-checked at compile-time.

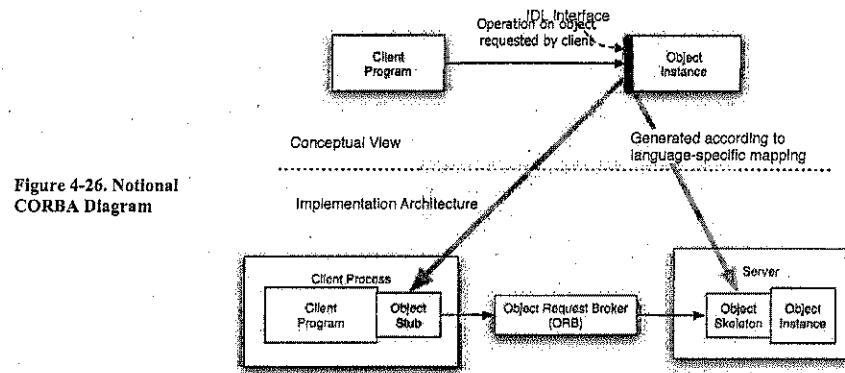


Figure 4-26. Notional CORBA Diagram

Figure 4-26 illustrates how CORBA connects objects across machine, language, and process boundaries. The top half of the diagram shows the conceptual, or logical view, which should be familiar to anyone who has written an object-oriented program. A client program obtains a pointer to an object that can perform a service for it, here labeled the 'object instance.' After obtaining this pointer, it makes calls on the object instance through one of its interface methods.

Within the context of a single programming language, in a single process running on a single machine, making an object call like this is straightforward. The pointer in this case is a direct memory reference, and the call represents a simple synchronous procedure call.

When language, process, and machine boundaries are involved, things become more complicated, and this is the problem that CORBA attempts to overcome. Implementations of CORBA are accompanied by tools called "IDL compilers" that can target specific platform and programming language combinations (e.g., C++ on Windows). When an IDL interface is run through an IDL compiler, two code artifacts are created, known as an "object stub" and an "object skeleton."

An object skeleton is an object in the target programming language/platform that provides empty implementations for each method defined in the IDL interface. IDL types are translated into local programming language types. The developer is then responsible for implementing these methods in the target programming language. These implementations make up the object instance, also known as the "true object."

The object stub is the complement of the object skeleton. It is an object that provides implementations for each method in the IDL interface, again in the target programming language. These method implementations do not actually perform the services provided by the true object, however. Instead, when a method on the stub is called, the calling parameters are encoded into a block of binary data in a process called ‘serialization’ or ‘marshaling.’ The stub then sends this block of data across machine or process boundaries, using a network or another inter-process communication (IPC) mechanism, to the object skeleton. The software that facilitates this is known in CORBA as the object request broker, or ORB. Depending on the CORBA implementation, this may be a separate piece of software, or it may be part of the stub and skeleton. The skeleton receives the call data, makes the corresponding invocation on the object instance, and then marshals the return value or exception for return to the stub. The stub then returns this data to the caller: the client program in the figure.

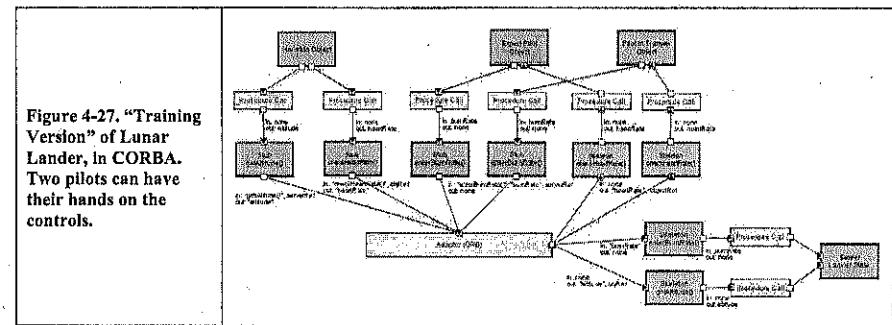
In this way, a client program can invoke a remote object without explicit knowledge that it is remote. From the client program’s perspective, the object stub is providing the service it needs. The object stub, however, is not really providing the service; it is sending the call data over the network to the skeleton, which calls the object instance—the true object—to perform the actual service. Data is returned by the same path in reverse.

The last part of the puzzle is how the client program/object stub pair obtain a pointer or reference to the object skeleton/object instance pair in the first place. This can be done in a number of ways, most commonly by a lookup or ‘naming’ service that maintains a directory of objects running on hosts and allows clients to look them up by name.

CORBA does the best it can to ensure that client and server object implementations are not aware that the call between them is traversing a language, process, or machine boundary. However, these boundaries can never be masked completely. There are two main differences between a local and a remote procedure call. First, all data that traverses a remote procedure call must be serializable. That is, the stub and skeleton must be able to transform the data into a block of binary data for transmission over a network. Parameters that contain pointers to arbitrary blocks of memory on the local machine or control objects like threads cannot be serialized, and thus cannot be passed or returned in a remote procedure call. Second, remote procedure calls suffer from a much wider variety of potential failures than local procedure calls. In a local procedure call, it is assumed that the call itself—the transfer of control and data from caller to callee—cannot fail. In a remote procedure call, network problems and dead processes can cause the call itself to fail. In these cases, a runtime

exception is raised by the call, but such exceptions would not have been expected in the context of a local procedure call. (Additional problems with network-based applications are discussed in Chapter 11.)

Although remote procedure calls are in some ways more limited and fragile than local ones, they can be more flexible as well. Calls can be redirected or logged by the object request broker without any changes to the client or server objects. New server objects and even new hosts can be dynamically created and come online during application run-time, and then be looked up by later clients. This imparts a measure of dynamism to applications built using CORBA.



**Figure 4-27.** “Training Version” of Lunar Lander, in CORBA. Two pilots can have their hands on the controls.

Figure 4-27 shows a simple application of CORBA in the design of a two-pilot “trainer” version of Lunar Lander. In this version, two independent user clients can view the state of the lander during its descent and both clients can adjust the fuel consumption rate. In addition, a third party client, which resides in Houston, monitors the state of the lander and the two client pilots. The state of the lander is maintained as a CORBA object on a remote server; the clients manipulate the burn rate by making calls, through the CORBA services. Each pilot client also maintains the state of the pilots. Thus, when Client Houston views the altitude of the lander, the request is routed to the server. However, when Client Houston views the heart rate of both pilots, the call is routed to both pilot clients.

The description here of CORBA has been quite brief, and the example simplistic. In practice, CORBA offers a very rich set of services for managing distributed objects and constructing sophisticated distributed architectures. Most CORBA implementations are accompanied by “CORBA services,” objects and interfaces that can be called to deal with object lifecycles, relationships, persistence, externalization, naming, trading, events, transactions, concurrency, properties, queries, security, licensing, versioning, notification, and so on.

Selecting CORBA as the basis for a software development project is a double-edged sword. On one hand, using CORBA allows systems to be implemented using components written in different languages on different platforms, and the CORBA middleware masks most of the differences automatically. For developers faced with integrating modern technologies with legacy systems, the allure is almost too good to pass up. However, using CORBA comes with a price. The use of CORBA provides these interoperability benefits, but it also induces applications to be built in the distributed objects style.

Distributed objects is not an ideal style for every application, and it has its drawbacks. For example, components in a distributed objects style are required to explicitly specify provided interfaces, but not to specify required interfaces. Objects in the CORBA world are constantly created, linked, unlinked, and destroyed. This makes it difficult to understand the configuration of a CORBA application at any given time. Distributed object interactions tend to be synchronous call-return, and many such systems have difficulty with asynchronous invocations or data that travels in streams.

The "Big Ball of Mud" architectural style has been described by Brian Foote and Joseph Yoder as the most common architectural style of all [80]. The style imposes no constraints, other than "get the job done." It offers the benefits of "We didn't have to think too much" and "It'll work for now, I hope." Software in the BBoM style is haphazard and thrown together. Such systems often grow by accretion: new bits of code are stuck onto pre-existing code to meet new demands, without discipline, plan, or care. The BBoM style is an important style for designers to keep in mind for one simple but critical reason: "If you can't articulate why your application is *not* a big ball of mud, then it is."

#### The Big Ball of Mud Style

#### 4.3.6 Discussion: Patterns and Styles

Taking a step back from the myriad of details associated with the styles and patterns discussed above, common characteristics are evident. Fundamentally, styles and patterns reflect experience and codify knowledge gained from that experience. Creating a good style entails reflection on experience, abstraction of the knowledge from the details, and possibly generalization. Thus styles are "refined experience in action".

Despite the fact that styles represent hard-won wisdom in system development, their use is sometimes resisted. Why? Because the very nature of styles, the adherence to a style during design, demands that the designer work within the set of constraints that comprise the style.

Somewhat the very notion of constraining the designer seems counterproductive and limiting. The curious, non-intuitive character of styles and designing, however, is that through the adherence to constraints, great freedom and effectiveness in design is achieved.

#### The Freedom of Constraints/ The Value of Invariants

When viewed as a set of constraints, styles limit the designer in several ways:

- The amount of detail or the number of concepts that the designer is allowed to deal with at any one time may be limited (e.g. in three-tier architectures);
- The way elements of the design are allowed to interact may be restricted (e.g. in event-based architectures, or in CORBA-based systems);
- There may be specific obligations on what particular elements must do – and not do (e.g., requiring inter-component communication to be strictly mediated by first-class connectors);
- The style may constrain the solution of some sub-problems to be addressed in a less than optimal way (for instance, pipe and filter always requires character stream communication, even when complex data structures are communicated). In such a case the benefits of consistent style, with its understandability and ability to be reused in standard, expected ways – outweighs any other limited benefit.

Where then does the "freedom" and effectiveness of styles come from? Numerous sources are apparent:

- Styles restrict ones focus, and thus creates a space of issues that the design does not have to be concerned about. (The styles free up thought space and directs attention to the essentials)
- Styles guarantee the applicability of particular analysis techniques.
- The constraints enable the use of code generation and framework implementation strategies – since patterns of interaction are regularized they can be automatically and/or efficiently supported in standard ways;
- Styles provide invariants – assertions that the designer can always count on ("as long as I follow the rules then I know the following must be true");
- Styles make communication more efficient: once project members know the rules, they form a baseline for communicating the added-value details;
- Similarly, styles promote understanding of design decisions after the fact, such as when the software is taken over by a new development team.

### Combination, Modification, and Creation of Styles and Patterns

While studying the long list of architectural styles in the preceding pages may have been exhausting, the list is certainly not exhaustive. A point we have stressed is that styles capture experience and distill it to an essence which is useable in new development situations. Seen this way, each application domain may have a specific style associated with it. More commonly, however, styles appropriate for a particular domain will be aggregations or combinations of simpler styles.

The combination of styles is motivated by the desire to obtain multiple benefits in design. A good example of a composite, and specialized style, is the C2 style discussed in Section 4.3.5. C2 is a combination of model-view-controller, layered systems, and event-based styles. An even more complicated example will be discussed in Chapter 11, namely REST. REST, of course, was introduced at the beginning of Chapter 1, but was discussed there without reference to how it was developed. The discussion in the later chapter will show how it drew ideas from several simpler styles and ideas.

Knowing that styles can be combined, specialized, or developed from scratch leads to the danger of creating new styles unnecessarily, or unwisely. Any designer could claim, with some justification, that his experience is what matters most to him, and hence codification of a style that represents that experience is important. Keep in mind, however, that one's own experience needs to be traded off against the aggregate experience of other designers within a company or application domain. Moreover formulation of yet-another-architectural-style (YAAS, indeed) negates one of the advantages of styles: the promotion of effective communication between designers. The lures of expediency and "good enough" seldom outweigh the genuine benefits of carefully applying established, well-known styles.

If after consideration of substantial experience, a group decides to formulate a new style to capture that experience and their insights, it should be done with an eye to capturing only what is truly central, and avoiding incidental matters. "Less is more" until adequate validation is obtained for the newly formulated approach. An important goal for such an exercise should be a clear articulation of what invariants are gained as the result of adding constraints.

A summary of the styles considered in this chapter appears in Figure 4-28.

Figure 4-28. A comparison table of architectural styles

Style Category & Name	Summary	Use It When	Avoid It When
-----------------------	---------	-------------	---------------

<i>Language-influenced styles</i>			
Main Program and Subroutines	Main program controls program execution, calling multiple subroutines.	Application is small and simple.	Complex data structures needed. Future modifications likely.
Object-oriented	Objects encapsulate state and accessing functions	Close mapping between external entities and internal objects is sensible. Many complex and interrelated data structures.	Application is distributed in a heterogeneous network. Strong independence between components necessary. High performance required.
Layered Virtual Machines	Virtual machine, or a layer, offers services to layers above it	Many applications can be based upon a single, common layer of services. Interface service specification resilient when implementation of a layer must change.	Many levels are required (causes inefficiency). Data structures must be accessed from multiple layers.
Client-server	Clients request service from a server	Centralization of computation and data at a single location (the server) promotes manageability and scalability; end-user processing limited to data entry and presentation.	Centrality presents a single-point-of-failure risk; Network bandwidth limited; Client machine capabilities rival or exceed the server's.
<i>Data-flow styles</i>			
Batch sequential	Separate programs executed sequentially, with batched input	Problem easily formulated as a set of sequential, severable steps.	Interactivity or concurrency between components necessary or desirable. Random-access to data required.
Pipe-and-filter	Separate programs, a.k.a. filters, executed, potentially concurrently. Pipes route	[As with batch-sequential] Filters are useful in more than one application. Data structures easily serializable.	Interaction between components required. Exchange of complex data structures between components required.

		data streams between filters
<b>Shared memory</b>		
Blackboard	Independent programs, access and communicate exclusively through a global repository known as blackboard	All calculation centers on a common, changing data structure; Order of processing dynamically determined and data-driven.
Rule-based	Use facts or rules entered into the knowledge base to resolve a query	Problem data and queries expressible as simple rules over which inference may be performed.
Interpreter	Interpreter parses and executes the input stream, updating the state maintained by the interpreter	Highly dynamic behavior required. High degree of end-user customizability.
Mobile Code	Code is mobile, that is, it is executed in a remote host	When it is more efficient to move processing to a data set than the data set to processing. When it is desirous to dynamically customize a local processing node through inclusion of external code
<b>Implicit Invocation</b>		
Publish-subscribe	Publishers broadcast messages to subscribers	Components are very loosely coupled. Subscription data is small and efficiently transported.

Event-based	Independent components asynchronously emit and receive events communicated over event buses	Components are concurrent and independent. Components heterogeneous and network-distributed.	Guarantees on real-time processing of events is required.
Peer-to-peer	Peers hold state and behavior and can act as both clients and servers	Peers are distributed in a network, can be heterogeneous, and mutually independent. Robust in face of independent failures. Highly scalable.	Trustworthiness of independent peers cannot be assured or managed. Resource discovery inefficient without designated nodes.
<b>More complex styles</b>			
C2	Layered network of concurrent components communicating by events	When independence from substrate technologies required. Heterogeneous applications. When support for product-lines desired.	When high-performance across many layers required. When multiple threads are inefficient.
Distributed Objects	Objects instantiated on different hosts	Objective is to preserve illusion of location-transparency	When high overhead of supporting middleware is excessive. When network properties are unmaskable, in practical terms.

## Design Recovery

So far we have discussed situations in which an architect has, or has access to, prior experience in designing a particular kind of system for an understood domain. If this is not the case, the problem faced by the architect falls in the province of unprecedented design. However, before we consider approaches for dealing with unprecedented design, we will consider one more source of experience—design recovery.

Different software design methods, discussed above, clearly differ in the details of how developers arrive at a software system. However, to one extent or another, they all rely on the assumption that a software project commences with some form of requirements gathering and specification, reaches its major milestone with system implementation and delivery, and then continues, possibly indefinitely, into an operation and maintenance phase. The software system's architecture is in many ways the linchpin of

this process: it is supposed to be an effective reification of the system's technical conception and to be faithfully reflected in the system's implementation. Furthermore, the architecture is meant to guide system evolution, while also being updated in the process.

Sadly, for many systems this turns out to be an idealized picture. Some systems are "hacked", without careful consideration or documentation of architectural concerns. Other systems are designed carefully and those initial designs documented, but repeated modifications are subsequently made with little concern for maintaining intellectual coherence, resulting in substantial architectural erosion. Software evolution certainly requires in-depth understanding of an application, its complexity, its overall architecture, its major components, and their interactions and dependencies. Unfortunately, many of these requirements are often ignored, with a frequent willingness to compromise the quality and longevity of a system in order to, for example, decrease its time-to-market. This attitude, coupled with the complexity of the involved systems and the sloppiness with which the changes to them are often documented, directly contributes to numerous recorded cases of architectural erosion.

Evolving a system with an undocumented, or documented but degraded, architecture poses tremendous challenges to engineers. It results in a real danger that the modifications intended to provide new functionality will be implemented incorrectly and those intended to remove a particular problem in the existing system will cause other, unforeseen problems. To deal with this issue, researchers and practitioners have typically engaged in architectural recovery, a process whereby the system's architectural design is extracted from its other artifacts, which are likely to be updated more reliably than the design itself. These artifacts may include requirements, formal specifications, test plans, and so on. However, most frequently design recovery uses a system's implementation as the starting point.

Simply put, then, the task of design recovery is one of examining the existing code base—both source code and possibly binary files for any externally developed functionality that is reused off-the-shelf—and determining what the system's components, connectors, and overall topology are. As with other architectural tasks, the goals of recovery will be viewpoint-specific.

A common approach to architectural recovery is *clustering* of the implementation-level entities into architectural elements. Based on the approach used for grouping source code entities, such as classes, procedures, or variables, software clustering techniques can be divided into two major categories: *syntactic* and *semantic* clustering.

Syntactic clustering focuses exclusively on the static relationships among code-level entities. This means that the design recovery activity can be performed without executing the system. The functional characteristics or meaning of the code-level entities are not taken into consideration. Instead, the entities are grouped together based on naming conventions or the existence of particular relationships between them. For example, if source code analysis shows that one class is encapsulated inside another, the two classes can be grouped together to represent (a part of) a single system component. More examples of relationships of this kind include variable and class references, procedure calls, use of packages, association and inheritance relationships among classes, and so on. In addition, syntactic clustering approaches can embody inter-component (a.k.a. coupling) and intra-component (a.k.a. cohesion) connectivity measures.

The major drawback of syntactic clustering is that it may ignore or misinterpret many subtle relationships and interactions among the implemented system's entities. This is particularly the case with *dynamic* information, such as the interaction frequency between two classes or the actual method invoked in the case of polymorphism. This problem is remedied by semantic clustering, which includes all aspects of a system's domain knowledge and information about the behavioral similarity of its entities. This means that all implementation constructs with similar functionality can be grouped together to form a software component. For example, all classes that provide support for checking the users' authenticity can be clustered into a single component. Although this approach may provide more meaningful components, it requires interpreting the system entities' meaning, and possibly executing the system on a representative set of inputs. In order to infer the necessary information, semantic clustering may also require that the system be instrumented and monitored during execution. Another potential difficulty is that semantic clustering techniques tend to be domain- or application-specific, so that their rules cannot be easily applied to an arbitrary system.

Note that, even if correct and complete structural and behavioral information about the system were available to a clustering technique, another key challenge that remains is recovering design intent and rationale. For example, it may not be obvious which of the recovered architectural elements were meant by the system's designers to play a central role in the system. This information may be obscured by the implementation. It may also depend on the architectural style(s) used to guide the system's initial design; at the same time, it may not be clear from the implementation what those styles were and whether they are still appropriate. Without this information, it may be difficult to separate essential characteristics of the system from the less critical and even accidental ones.

An excellent example of fine work in performing architectural recovery is given by the Apache Modeling Project at the Hasso-Plattner-Institute for Software Systems Engineering in Potsdam, Germany. The recovery effort focused on the Apache HTTP server, which is the most widely used HTTP server world-wide. The project used the "Fundamental Modeling Concepts (FMC) approach." The high quality of the work done and the documentation produced is attested by praise given to the project by the Apache developers – who were not involved in the recovery project. Details can be found at [103].

A similarly excellent recovery project focused on the Linux operating system, and compared its recovered architecture with its prescriptive architecture [26].

#### 4.4 Architectural Conception In Absence of Experience: "Unprecedented" Design

The primary focus of this chapter up to this point has been to indicate how to identify a feasible set of "alternative arrangements for the design as a whole" through the application of experience. Refined experience as codified in architectural patterns and styles has been a major focus, since they are so broadly and commonly useful. Even when experience has not been codified, it may still be found in pre-existing systems, hence the above discussion of design recovery. Novel design challenges do exist, however. As Jones [145] (pg. 24) says, "... the principle of deciding the form of the whole before the details have been explored outside the mind of the chief designer does not work in novel situations for which the necessary experience cannot be contained within the mind of one person." At a minimum, if a designer is ignorant of relevant experience, for that designer the new problem is indeed a novel one.

It should be obvious that the first effort a designer should make in addressing a novel design challenge is to attempt to assure himself that it is genuinely a novel problem. The cost differences are the reason: if experience can be applied a much quicker and cheaper route to a solution is available. One risk is the "siren song of novelty". Tackling novel problems is fun; the added challenge and the opportunity to display creativity is a winsome combination. So, be careful to assess a problem carefully ... the sheer delight of a new problem can be enjoyed most delectably if the novelty is indeed genuine.

Assuming that the designer has made a good faith effort to map a new problem to existing solution strategies and has concluded that the problem

presents sufficient differences to demand a "green field" effort, a variety of techniques are available to assist the designer. The essence is to adopt a design strategy, and to control that strategy. Below we discuss the overall strategy in broad terms and then consider a few specific techniques. The section concludes with remarks about controlling the process.

##### Basic Strategy

Failure to meet the needs of a new design challenge with approaches based upon past experience demands a rethinking of the problem and approaches to its solution. The multitude of authors who have discussed this situation – which exists in all fields of design, whether software focused or not – essentially recommend the following process:

1. Divergence
2. Transformation
3. Convergence

*Divergence* is a step taken to shake off the confines of inadequate prior approaches and discover, or admit, a variety of new ideas, conceptions, and approaches which offer the promise of a workable solution.

*Transformation* is a combination of analysis and selection: based upon the information from the Divergence step, solution possibilities and new understandings of or changes to the problem statement are examined and formulated.

*Convergence* is the step of selecting and further refining ideas until a single approach is selected for further detailed development.

As Jones puts it, "... the aim of divergent search is to de-structure, or to destroy, the original brief while identifying these features of the design situation that will permit a valuable and feasible degree of change. To search divergently is also to provide, as cheaply and quickly as possible, sufficient new experience to counteract any false assumptions that the design team members, and the sponsors, held at the start." (page 66)

There are both difficulties and risks in the critical first step. One difficulty is simply breaking free from prior understandings and approaches to the problem area. The desire to cling to the old tried-and-true approaches is common both in individuals and in organizations. The old approaches were the basis for whatever success the person or company has achieved to date, so moving into new territory will likely be viewed skeptically. Examples abound in ordinary life: whether the topic is new transportation systems, medical treatments, or communication technologies, new approaches often have difficult entry into practice.

The flip-side risk of not adequately stepping away from better understood approaches and techniques is not anchoring “wide exploration” in assessments of costs and benefits. Suppose one hundred new solution possibilities emerge from the divergence step. Should all be explored fully, to determine which one is best? Supposing one thousand possibilities emerge? The key is that the designer must make realistic judgments of the magnitude of the perceived penalties for *not* exploring a given alternative. The cost of analyzing a given approach must not exceed the value obtained by performing the analysis.

Yet another risk is tunnel-vision: a novel approach is explored which breaks sharply from previous practice, but enthusiasm for this one approach stifles any attempt to also explore other novel alternatives. It is a difficult balance.

While much has been written about the activity of design and creative processes, most of that literature has come from the industrial design community or from academics. It is interesting to see how individuals who come from entirely different backgrounds come to very similar conclusions. John Boyd was a fighter pilot in the U.S. Air Force in the 1950's, who went on to designing combat tactics, then combat aircraft, and ultimately to wide-scale military strategy. Towards the end of his long career he wrote an essay entitled “Destruction and Creation” which addresses the issue of designing solutions for novel problems. He formulated his approach as a two-step process:

- (1) Destruction/unstructuring/destructive deduction
- (2) Synthesis/restructuring/creative induction

He summarized these as follows:

“Also, remember, in order to perform these dialectic mental operations we must first shatter the rigid conceptual pattern, or patterns, firmly established in our mind. (This should not be too difficult since the rising confusion and disorder is already helping us to undermine any patterns). Next, we must find some common qualities, attributes, or operations to link isolated facts, perceptions, ideas, impressions, interactions, observations, etc. together as possible concepts to represent the real world. Finally, we must repeat this unstructuring and restructuring until we develop a concept that begins to match-up with reality.” (John Boyd, “Destruction and Creation”, reprinted in [47])

The additional insight shown here, as compared to the three-step process in the main text, is the focus on repeatedly cycling through the activities of “destruction” and synthesis, until a feasible solution emerges. Note as well the implied focus on understanding and formulating the problem in new terms and in new ways.

A Fighter Pilot on Design:

### Detailed Strategies

Numerous detailed strategies for helping a designer tackle a novel problem have been articulated in books and articles over a long period of time. Most strategies are very general and are appropriately focused on the “divergence step”. They are not specific to software development. This does not diminish their utility however, as cookie-cutter solutions are by their very nature insufficient for novel situations. The need for creative, deep thought will be uncomfortable and unpleasant for some, but delightful for others.

Below we discuss several specific strategies. Jones [145] catalogs thirty-five techniques; we have selected and adapted a few of the most relevant for use in the software engineering context.

### Analogy Searching

The idea of analogy searching is to examine other fields and disciplines unrelated to the target problem for approaches and ideas that are analogous to the problem at hand, and formulate a solution strategy based upon that analogy.

A common “unrelated domain” that has yielded a variety of solutions is nature, in particular the biological sciences. One arguable success from this approach has been neural nets: from understanding of how neural networks work in “wetware”, i.e. the neural systems of animals, ideas are offered for structuring software systems to parallel process certain types of data. Other domains have offered solution ideas such as flow architectures: whether the inspiration was sewage systems, circulatory systems, or postal mail systems, a variety of software systems have flow structures and characteristics which reflect our common understanding of these physical systems.

Jones' discussion of analogy searching identifies four types of analogies: direct, personal, symbolic, and fantasy. The examples in the preceding paragraph are direct analogies: a concept in the domain of the analogy has a correspondent in the design domain. Personal analogies are rather different; to quote Jones, “The designer imagines what it would be like to use one's body to produce the effect that is being sought, e.g. what would it feel like to be a helicopter blade, what forces would act on me from the air and the hub, ...” While this type of analogy may initially seem to have limited usefulness in the domain of software architecture, one might consider its use in the development of intelligent systems that interact frequently and via various modes with a human user. Symbolic analogies focus on metaphors and similes “in which aspects of one thing are identified with aspects of another”. Perhaps the most obvious example of

this in the World Wide Web, and especially with the notion there of "broken links" – the image of a damaged spider's web is very evocative. Fantasy analogies are analogies to things which are "wishes". A good, and useful, example is a sky hook – a device for lifting which attaches to the object to be carried on one end and to the air on the other end. Fantasy analogies can help to temporarily simplify a problem such that the remaining parts can be more directly addressed. Naturally one does have to return to the fantasy part, but perhaps by then some feasible strategy will be identified.

As mentioned in the early chapters of this book, when talking about the architecture of buildings, every analogy has limitations and it is important to recognize when those limits have been reached. The utility of analogies is in providing rich sets of initial concepts for developing a solution to a design problem. Development of the details can proceed in absence of further consideration of the analogy.

#### *Brainstorming*

Brainstorming is the technique of rapidly generating a wide set of ideas and thoughts pertaining to a design problem without (initially) devoting effort to assessing the feasibility, desirability, or qualities of those ideas. After the ideas are generated then a period of categorization and analysis of the results can begin. Brainstorming can be done by an individual or, more commonly, by a group. The primary association of groups with brainstorming is based on the belief that expression of an idea by one individual in a group will trigger a creative response from another. As a strategy it is well known.

As many people who have participated in brainstorming sessions have observed, however, potential problems with the technique are numerous. A brainstorming session can generate a large number of ideas... all of which are low-quality. Sessions can degenerate into "coblabboration" or "blamestorming", to quote Harvard's David Perkins.

Successful brainstorming appears to require advance planning and careful management. Having people come to the session with a set of ideas already prepared and written can speed the process, remove awkwardness, and provide some "egoless" participation. The use of external facilitators (meeting supervisors) can help keep the discussion focused and avoid personality-based clashes. Jones' view is that the chief value of brainstorming is in identifying *categories* of possible designs, not any specific design solution suggested during a session. After a group brainstorming session is over, individuals may continue the process on their own, or design process may proceed to the Transformation and Convergence steps.

#### *"Literature" Searching*

The classic design disciplines have used literature searching – the process of examining published information to identify material that can be used to guide or inspire designers – for decades. The advent of the Web, the ability to search electronically, and the availability of free or open-source software has breathed new life into this approach, however, making it especially useful.

Not only are all the historically useful ways of searching "literature" available, but digital library collections make searching extraordinarily faster and more effective. For software designers the availability of the ACM Digital Library and IEEE Xplore offer a world of insightful, deep literature. More generally Google, Google Scholar, and other search engines offer the ability to examine a phenomenal base of information.

The importance of these digital resources is all the more important since all too often practitioners live in a very small world with very limited ability to interact with practitioners from other companies or with researchers – those people whose careers are devoted to investigating novel problems. There's always enough time for yet-another-group-meeting or sensitivity-training seminar, but never enough time to read a technical magazine, attend a conference, or take a professional development seminar. Digital library resources offer some respite from this isolation.

The availability of free and open-source software adds special value to this technique. Even if a direct solution to the problem at hand is not freely available, the designer may be able to devise a solution composed of large pieces of pre-existing software – perhaps composed in a manner totally unanticipated by the original developers.

Lastly, developers should not overlook the use of the patent database as a source of ideas, approaches, and inspiration. While learning to read a patent takes a bit of time, the astounding wealth of ideas in the world's patent databases makes them valuable electronic resources.

#### *Morphological Charts*

The essential idea of morphological charts is to (1) identify all the primary functions to be performed by the desired system, (2) for each function identify a means of performing that function, and (3) then attempt to choose one means for each function such that the collection of means performs all the required functions in a compatible manner. Put another way, the problem is subdivided into parts, a solution for each sub-part is devised, then (hopefully) a solution for the whole is created by combining the sub-solutions to the various parts. The trick, of course, is that the

functions and sub-solutions need to be independent and compatible with each other. If the functions, or their sub-solutions, are not independent then the designer is bound to consider the functions together. If the chosen sub-solutions are not mutually compatible, then another combination of sub-solutions must be examined.

At first glance this technique seems to be nothing more than a fancy name for the old, and somewhat discredited, top-down design. Its value, however, derives from the fact that the technique does not demand that the functions be shown to be independent when starting out; similarly there is no *a priori* requirement for the sub-solutions to a given problem be developed under the constraint of being compatible with all the sub-solutions to other functions. Recall the overall aim: divergence – the technique offers help in constructing a variety of approaches to parts of the overall problem. During the transformation step the functions and their sub-solutions may be reshaped such that ultimately, during the convergence phase, a compatible solution is devised.

#### *Removing mental blocks*

Getting stuck on a problem is nothing new. It is no surprise, then, to hear that many mental strategies have been promulgated for aiding the designer. Perhaps chief among these is transformation: for instance, if you can't solve the problem, change the problem to one you can solve. If the new problem is "close enough" to what is needed, then closure is reached. If it is not close enough, the solution to the revised problem may suggest new venues for attacking the original.

A variety of transformation strategies are available, many of which can be seen and applied in software architecture. Elements of a solution may be adapted, modified, substituted, re-ordered, or combined to offer new structures.

Jones advocates a strategy of reassessing the design situation. This gets somewhat to the issue of tunnel-vision as mentioned above, but has broad utility. "Matchett's insistence ... upon continually returning to the 'Primary Functional need' (that which *must* be satisfied if the design is to be accepted) is probably the most reliable way of side-stepping a difficulty. In most cases the designer will be reminded that the sub-problems are of his own choosing and that he can satisfy the Primary Functional Need with an entirely different set of sub-needs if he changes his view of the problem." Or indeed, if the problem itself is changed.

Additional strategies are detailed in Stephen Albin's book, "The Art of Software Architecture" [6] and other references provided at the end of the chapter.

#### **Controlling the Design Strategies**

The potentially chaotic nature of exploring diverse approaches to the problem demands that some care be used in managing the activity. If the search for novel solutions is unconstrained, a great deal of time and money can be wasted. This suggests the following four guidelines (two of which are adapted from Jones):

1. Identify and review critical decisions (i.e., perform risk analysis). By identifying the critical issues, and the consequences of choices regarding those issues, the designer's focus can be kept on-track.
2. Relate the costs of research and design to the penalty for taking wrong decisions; "the penalty for not knowing must exceed the cost of finding out". Making a wrong decision may not be the end of the world; if the issue is not of great consequence, then a sub-optimal approach may be acceptable. To keep making progress it can be necessary to make a decision, even a potentially poor one, to enable all issues to be surfaced and addressed.
3. Insulate uncertain decisions. Decisions for which the design is unsure, or for which the circumstances dictating the issue may change, argue for carefully insulating that decision from the rest of the design. This is the standard dictum of software engineering due to David Parnas: matters likely to change should be encapsulated inside boundaries (such as a component with resilient interfaces) so that when change eventually does come, the rest of the system is unaffected. (This is analogous to the concept of shearing layers in building architecture, a topic discussed later, in Chapter 14.)
4. Continually re-evaluate system "requirements" in light of what the design exploration yields. It is the rare system whose requirements are genuinely firm and which cannot be improved, or changed, as the result of divergent design explorations. Costs for meeting requirements must be re-examined, and opportunities for novel, unanticipated functionalities should be pursued.

## **4.5 Putting it All Together: Design Processes Revisited**

This chapter has presented a wide range of concepts and techniques for use in the design of software architectures. They have ranged from the very basic – reminders to use abstraction and separation of concerns – to extensive treatment of architectures, styles, and patterns which encapsulate knowledge gained from experience with many prior systems. The chapter has also presented approaches for designing in situations where there is little or no experience upon which to draw.

Faced with a new development task, system architects must sort through all the issues confronting them, choose a design approach, and see it

through. As we noted at the beginning of this chapter, the central task is choosing a feasible set of concepts upon which to build the design, then progressively refining and revising the concepts and the ensuing details until a satisfactory architecture is developed.

Perhaps the hardest part of the whole process is knowing whether to attempt to base the new design on some existing design – i.e. use the “Grand Tool of Experience”, or to approach the design task as one that is unprecedented. Whether an application presents novel challenges or not, significant insight can come from iteratively working with requirements for the system. Hence below we call to mind a few thoughts that were introduced in Chapter 2, and expand upon them briefly. Implementation concerns can also further shape and guide the design process, hence we include below a short section dealing with that topic.

A comprehensive methodology for applying all these concepts such that any arbitrary problem can be tackled in a straightforward manner is beyond the scope of this text – indeed, beyond what anyone has yet credibly set forth. The design process — a good design process— will take many twists and turns after the initial attempt at concept formation. But that's part of the fun. You get to be creative.

#### 4.5.1 Insights from Requirements

Chapter 2 pointed out the intimate relationship between requirements engineering and software architectures. Pre-existing architectures provide a frame of reference for developing new requirements statements.

Architectures provide

- a vocabulary – not just of basic concepts, but of means, approaches, and possibilities;
- a framework for describing properties (e.g., by describing relationships between structural elements, or by categorization of types of design decisions);
- a basis for analysis (e.g., through knowledge of previous design decisions and their consequences one can assess possible consequences of new requirements).

In many cases – perhaps most – new architectures can be created based upon experience with pre-existing architectures and improvement to them.

Restated, the organic interaction between past design and new requirements means that many critical decisions for a new design can be identified or made.

- Experience can show what the most critical issues are, or what the most difficult problems are likely to be.
- Experience can suggest what the key levels of discourse are, and what vocabularies to use in each.

- Experience can show successful patterns of product specialization.
- Experience can show what architectural patterns and styles have been effective in this domain.
- Experience can show areas in which novel development has typically been required.

One aspect of this iterative conceptualization of the new application is in the identification of “tipping points” – decisions which have profound consequences for the rest of the design and implementation. An important example is deciding whether part or all of the new application should be created as a modification of an existing system. This can be a very difficult choice: modifying an existing system offers the potential of achieving substantial software reuse, with attendant cost and schedule benefits. Yet a time comes in the evolution of every system when achieving new requirements demands more of the pre-existing architecture than it can bear, and hence an entirely new design is called for. Core algorithms, for example, may not be capable of scaling to new performance requirements, thus requiring a new approach.

All of these are important aids in getting started with the design of a new application; they derive from the symbiosis between articulating new requirements using a vocabulary of known architectural choices.

In those rare cases where a requirements specification is used that does not make any reference to existing architectures, careful analysis is required to identify the critical factors, to distinguish between the incidental and the essential. A highly dynamic approach to the first critical steps of identifying “a set of alternative arrangements for the design as a whole” is required in such cases. Several such approaches were identified at the end of Section 4.1. You may need to attempt to design a solution using several different structures, applying various styles from the discussion in Section 4.3, then compare the results and the properties obtained, in order to determine the best course to take.

Many touted design strategies are simply transformations of requirements into, in effect, simulations of some part of the real world. As such, the architecture is determined simply by the domain and particular manner of stating the requirements, and not by thoughtful, creative design or the use of sound software design principles.

One example is the “Underline the nouns, underline the verbs” approach to design first promulgated in [4]. The essence is that the identified nouns determine a program’s data types (objects), the verbs become the names of the methods defined on those noun-objects. This approach to object-oriented design was popularized widely by Grady Booch. In [22] he says,

"Since we are dealing with a philosophy of design, we should first recognize the fundamental criteria [sic] for decomposing a system using object-oriented techniques. *Each module in the system denotes an object or class of objects from the problem space.*"

A similar tack was taken in the Jackson System Design (JSD) method: "From the late 1970s to the second half of the 1980s I worked with John Cameron and others on the JSD Method of analysis and design for information systems. The method is based on separating the construction of a model (for example, in a database) of the real world from the construction of the information functions that extract and display the necessary information from the model. The model focuses chiefly on the behaviours of real-world entities over their lifetimes, representing each entity as one or more sequential processes; the local variables of these processes form the data part of the model of the entity. The method is described in my book *System Development*." [14]

#### 4.5.2 Insights from Implementation

A detailed discussion of techniques and approaches to use when moving from an architecture to an implementation is found in Chapter 9. Here we look at the feedback situation: how information and insights from the implementation domain, or from constraints on that activity, can or must be used in development of a detailed architecture.

First, constraints on the implementation activity may help shape the design. Externally motivated decisions may be principal, and hence be a part of the architecture. For example, external constraints may dictate the use of a particular type or brand of middleware (connector technology). A large project focused on software-defined radios, for instance, mandated the use of CORBA, even before any detailed designs for the radios had been completed. Accommodating such mandates can dramatically affect the system's architecture – and not always for the better.

Similarly, externally motivated constraints may dictate the use of particular programming languages, development environments, or implementation platforms. The skill set of the staff devoted to the implementation may be limited. These, and other similar constraints, can shape the architecture, perhaps restricting the set of architectural styles that may be used.

A more interesting impact on design may come from considerations of software reuse. The potential cost savings from reusing software –

whether internal to the development organization or from free/open source sites – are substantial. But imperfect correspondence between the available software with the prescriptive design can require design modifications. Mismatches possible include functionality (the desired function is not there, but a similar one is), interface (the desired functionality is present, but the manner of invoking it is different from the current design), and non-functional properties (e.g., the desired functionality and the desired interface is present, but it runs too slowly or requires too much memory, or has inadequate security features).

Presence of such a situation invites an iteration between the design process and the implementation activity. The most effective course of action may in fact be to change the design to enable easier reuse. The decision of whether to reuse code and the manner in which it should be used (e.g. encapsulated, or modified) is a principal design decision grounded in implementation issues, and hence must be considered during the design process.

Just as development of requirements and development of design must proceed cooperatively and contemporaneously, so too may design and implementation. Initial implementation activities may yield critical performance or feasibility information, allowing the designer to proceed with confidence in other aspects of the system's design. At all costs architectural erosion must be prevented.

#### 4.6 End Matter

Designing architectures is the occasion when the designer can most obviously employ and exhibit all his innate creativity and talent. Designing well is a skill to be learned and practiced. It requires being willing to take some risks, explore some dark alleys, and occasionally backtrack. Timid, staid approaches may yield software that satisfies most requirements, but seldom will yield applications that give satisfaction to the user and enable the designer's organization to dominate the marketplace.

The most effective approaches to design will be those which have been refined and seasoned within the domain of the new application. Knowledge of effective design techniques and tradeoffs is an important corporate asset; ensuring that such knowledge is shared amongst projects and between designers should be an important managerial goal.

##### The Business Case

The essential business case for design is: "What's the alternative?" Creating products that are successful in the marketplace, effective to

maintain, and which lead to future successful products demands a thoughtful approach to product design. Design of product families – such as the consumer electronics example discussed several places – is a key means for assuring corporate growth through an expanding range of economically achieved products.

Additionally to designing the software's structure, a company must equally deliberately design a product's user interface, interaction behavior, and "feel". Design of these domain-specific characteristics must proceed cooperatively with design of the software structures that implement them, a theme first emphasized in Chapter 2.

A company's design processes represent a central asset of an organization. The successful and efficient production of new products is at the heart of a company. Design carries corporate value, and processes and traditions outlive most products. Given inevitable turnover of personnel, maintenance of good design processes depends upon production of explicit designs and articulation of the rationale behind the design decisions underlying them.

Since designing is a central asset it should be no surprise that it is an activity that cannot be "off-shored". Good design demands interaction with marketing, customers, domain experts, and business analysts. Once a design has been fully elaborated to crisp, low-level specifications, their implementation becomes a candidate for out-sourcing, but even then caution is in order. The designers must be able to assure themselves that no principal design decisions will be made during implementation – and that can be a very difficult assurance to achieve.

Given the importance of designing to an organization, the training and development of designers throughout the organization should be a continual priority. If an organization sinks to state where one or two "master designers" are allowed to dominate development, the organization becomes at risk. Design is teachable and is not the exclusive province of an elite few.

## 4.7 Review Questions

14. How can experience be used as a "design technique"? What must be true about "experience" in order for it to be useful in the design of a new system?
15. Refined experience, in the form of architectural styles, for example, can appear and be applied at different levels of abstraction and at different degrees of domain specificity. What are some examples of

different "styles" at different points in this space of abstraction and domain-specificity?

16. What types of applications are appropriate for the following styles? Alternatively, describe an example application for each of the following styles: event-based, pipe-and-filter, layered, mobile-code.
17. Describe a good process for designing an application for which the development team has no prior experience in the domain of the application and no prior architecture or code from which to work.

## 4.8 Exercises

1. For many years design by step-wise refinement was viewed as an appropriate, effective strategy for program development. Today it is viewed as quaint and inadequate. Explain what's wrong with the concept of step-wise refinement in the context of modern complex systems development.
2. Suppose an application has been in use by an organization for twenty years. It has been modified and expanded over that period to meet a steady stream of new demands. Now a new set of demands arise, requiring further changes. The software engineers in charge of the application are apprehensive about attempting to further modify the system to meet the new needs. How should the team decide whether to continue to try to modify the existing system, or build a new application from the ground up?
3. Top-down or bottom-up? Under what circumstances would it make the most sense to attack the design problem for a large project by working initially on sub-parts of the problem – without being sure that any sub-assembly so designed would end up as part of the final design solution?
4. The numerous examples of designs for the lunar lander in the chapter are all "sketches" in that they do not include the details of how the various components communicate. Elaborate the lunar lander designs to the next level of detail, such that the designs could be handed over to a coder for final implementation. Assume a textual user interface. State the assumptions made by the game in each example with regard to the use (or not) of a clock.
  - i. Layered architecture
  - ii. Sense-compute-control as main-program-and-subroutines
  - iii. Object-oriented
5. Describe the architecture of a compiler in terms of architectural styles. Is it a single style as found in this chapter? Multiple styles composed together?
6. What's the architecture of Microsoft Word? How can you tell? What would you need to see in order to know?
7. Examine the architecture of the Apache web server as characterized by the Apache recovery project [103]. What styles are involved, and how are they combined?

8. Examine the architecture of Linux, as characterized by Holt [26]. What styles are involved, and how are they combined?
9. Some designers have argued that “Powerpoint architectures” promote good design. In particular, that the discipline of working within a confined frame (e.g. the amount of space you have on a single Powerpoint slide) force the designer to apply abstraction and hierarchy. Discuss the pro’s and con’s of Powerpoint architectures.

## 4.9 Further Reading

Design has been a topic of study outside of computer science and software engineering for many years. The book by Jones [145] cited several times in this chapter is an excellent example of insight about the design process as seen from the industrial design perspective. A revised version was issued in 1992 [146]. A more recent book, focusing on group and corporate process, comes from the founders of the IDEO design firm, [149]

As mentioned at the end of Chapter 1, many excellent books on architectural design have been written, of course, but few provide substantive insights for software developers. Relative to this chapter, however, an important exception is Christopher Alexander’s *The Timeless Way of Building* [8] and a follow-on book, *A Pattern Language: Towns, Buildings, Construction*[7]. As mentioned earlier, his work has influenced thinking on patterns for object-oriented programming, and more generally, software architecture styles. Another key classic in the study of design is *The Reflective Practitioner* [253], by Schön, who characterizes design as an on-going conversation between the designer, the materials, and the context for the design.

A broad overview of *software* design as a research field – where it has been and where it is going – is found in “Software Design and Architecture: The once and future focus of software engineering” [277]. This paper includes a large bibliography of software design books and papers, and constitutes an important reference and starting point for detailed investigations.

The model-view-controller pattern was developed in the late 70’s; an original paper plus a retrospective can be found in [238, 239]. Numerous resources are available on the Web to further demonstrate its application. The mobile code styles are explored nicely in a paper by Fuggetta, Pico, and Vigna [83]. The C2 architectural style has been described and illustrated in the literature in several places, including [52, 188, 244, 275]. CORBA references abound. Perhaps the best introduction to the concepts is found in Emmerich’s book, *Engineering Distributed Objects* [69]. Abundant source materials can be found on the Object Management Group’s website ([www.omg.org](http://www.omg.org)).

Numerous resources are available in print and on-line, documenting and explaining the U.S. Apollo missions to the moon. Many of these resources are available directly from NASA as well as secondary re-publishers, and includes “Apollo 11 The NASA Mission Reports”. An excellent introduction to the on-board software and a recounting of the errors that were incurred and overcome during the Apollo 11 lunar descent can be found in [70].

## CHAPTER 5

# 5 Connectors

Designing and implementing the *functionality* and managing the *data* of modern large, complex, distributed, multi-lingual software systems is undoubtedly very difficult. As discussed in the preceding chapters, early software architectural models of system components, their key services, their abstract behaviors, and their non-functional properties are indispensable in this endeavor. However, experience has shown time and again that effectively *integrating* those components and ensuring their proper *interaction* to achieve the system's overall purpose is just as important, and can be even more challenging than the development of functionality. The particular importance in modern systems of mechanisms for assembling functional components and supporting their interaction, that is, software *connectors*, mandates that they be treated and studied separately. We will do just that in this chapter, and will return to this subject repeatedly throughout the remainder of the book.

Simply put, software connectors perform transfer of control and data among components. Connectors can also provide services, such as persistence, invocation, messaging, and transactions, that are largely independent of the interacting components' functionalities. These services are usually considered to be "facilities components" in widely used middleware standards such as CORBA, DCOM, and RMI. However, recognizing these facilities as connectors helps to clarify an architecture and keep the components' focus on application- and domain-specific information. Treating these services as connectors rather than components can also foster their reuse across applications and domains. Perhaps most importantly, connectors allow architects and engineers to compose heterogeneous functionality, developed at different times, in different locations, by different organizations. As such, connectors can be thought of quite appropriately as the guards at the gate of separation of concerns.

A common misconception about software connectors is that they are just "calls" between two components, in the manner of, say, a Java method invocation. A slightly more advanced view, inspired by middleware-based system development, is that component interactions take place via message passing and remote procedure calls (RPC). While it is frequently

the case that two components will eventually be implemented to communicate using, say, a Java method call, it is important to realize that as a software system's architect you are not restricted to assuming and relying on only such primitive interaction mechanisms.

Traditional software engineering approaches embrace a rather narrow view of connectors that is unlikely to be successfully applicable across all development situations. This problem is further exacerbated by the increased emphasis on development using large, off-the-shelf components originating from multiple sources. As components become more complex and heterogeneous, the interactions among them become more critical determinants of system properties. Experience has shown that integrating components with mismatched assumptions about their environment is hard to do and can lead to many problems. It is the task of connectors to mitigate such mismatches.

An architect has a wide range of connector options that are applicable, and often tailorable, to different development needs and scenarios. For example, he can choose to use a connector that distributes a service request to specifically named recipient components, or a connector that broadcasts a notification of a locally occurring event to any (unnamed and even unknown) component that may be interested and "listening"; the connector may require the sender component to suspend its processing until an acknowledgment of its request is received, or it may allow the sender component to continue with its processing; the connector can route each request in the order it received it, or it can try to order, filter out, or combine requests according to some pre-specified rule; and so on.

Therefore, a very important dimension of a software architect's job is to

- understand the component interaction needs,
- carefully identify all of the relevant attributes of that interaction,
- select the candidate connectors,
- assess any trade-offs associated with each candidate, and
- analyze the key properties of the resulting component-connector assemblies.

The goal of this chapter is to provide insights, guidelines, and specific techniques to support accomplishment of these tasks. The remainder of the chapter will introduce:

1. the different roles connectors play in a software system,
2. different connector types a software architect has at his disposal and the roles each type can fulfill,
3. a panoply of variation points for each connector type, and
4. a set of general hints and guidelines about a connector's applicability, strengths, and drawbacks.

Throughout the chapter, we will provide examples of specific software connectors to illustrate the discussion. The reader will probably be familiar with many of these connectors, although sometimes under a different name. The chapter starts off with a simple concrete example, to set the stage for the subsequent discussion.

This chapter provides a detailed treatment of connectors. The type and amount of information provided below is necessary for their thorough study. At the same time, some of the content may be unsuitable for an inexperienced reader. We recommend that all readers read at least Sections 5.1 through 5.4. Section 5.5 contains a set of examples from the domain of large-scale data distribution systems. These examples can be followed by most readers, but their full appreciation may require some prior experience with these types of systems. The remaining sections are appropriate for all readers, but in particular are targeted at the experienced professionals and readers interested in practical guidelines for constructing advanced connectors.

<b>Outline of Chapter 5</b>	5 Connectors 5.1 Connectors in Action – A Motivating Example 5.2 Connector Foundations 5.3 Connector Roles 5.4 Connector Types and their Variation Dimensions 5.4.1 Procedure Call 5.4.2 Event 5.4.3 Data Access 5.4.4 Linkage 5.4.5 Stream 5.4.6 Arbitrator 5.4.7 Adaptor 5.4.8 Distributor 5.5 Example Connectors 5.5.1 Event-based Data Distribution Connectors 5.5.2 Grid-based Data Distribution Connectors 5.5.3 Client-Server-based Data Distribution Connectors 5.5.4 P2P-based Data Distribution Connectors 5.6 Using the Connector Framework 5.6.1 Selecting Appropriate Connectors 5.6.2 Detecting Mismatches 5.7 End Matter 5.8 Review Questions 5.9 Exercises 5.10 Further Reading
-----------------------------	---

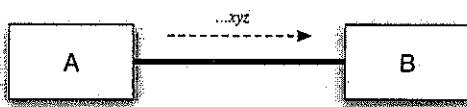
## 5.1 Connectors in Action – A Motivating Example

One useful property of connectors is that they are for the most part application-independent architectural elements. That means that they enable us to understand a lot about *how* a software system accomplishes its tasks without necessarily having to know exactly *what* the system does. In other words, connectors directly support two key principles of software engineering: abstraction and separation of concerns. Explicitly focusing on connectors also enables development and use of a specific vocabulary of software interaction. In turn, agreeing on appropriate terminology allows us to communicate easily and reason precisely about a number of software system properties that derive from the system components' interactions. To illustrate this, we will use a very simple example involving two different types of connectors. We will intentionally use the terminology associated with those connectors without defining it, to draw attention to this new “language”. The appropriate definitions and explanations will be given in the subsequent sections. Nonetheless, you will probably find that you are familiar with some, if not most, of this terminology.

Different views of a software connector are useful for different tasks. In order to model a system and communicate its properties, a high-level view is suitable. For example, an architect may make the following concise, but meaningful statement about the configuration shown in Figure 5-1: “Components A and B communicate via a Unix pipe.” That statement may be accompanied by a formal specification of the pipe’s overall behavior. However, such a high-level description does not help us understand all the properties of the pipe, how it can be adapted, or under what conditions it can be replaced with another type of connector. A more detailed, lower-level view is needed to accommodate that.

In particular, the pipe in Figure 5-1 allows interaction via unformatted streams of data. It is a simple connector: it consists of a single interaction channel, or *duct*, and facilitates only *unidirectional data transfer*. Thus, the cardinality of the pipe is a *single sender* and a *single receiver*. You will recall from the preceding chapters that a pipe allows components (that is, filters) A and B to exhibit very low coupling: the components do not possess any knowledge about one another. For example, A’s task is only to successfully hand off its data to the pipe; the actual recipient (if any) is unimportant to A. In turn, the particular pipe depicted in Figure 5-1 does not *buffer* the data. If attempts to *deliver* the data *at most once*; if the recipient is unable to receive the data for some reason, the data will be lost.

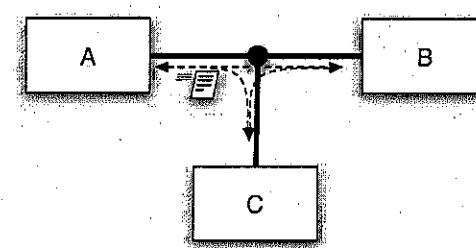
**Figure 5-1.** A simple pipe-and-filter architecture consisting of two filters, A and B, communicating via untyped data streams through the unidirectional pipe connector P.



Let us now assume that we need to alter the manner in which A and B interact, such that B can also send information (e.g., *acknowledgement* of data receipt) back to A. Furthermore, we wish to *ensure the delivery* of data: if the recipient is not available, the pipe *retries* to send until the data is successfully transferred. Both these modifications can be potentially accommodated by pipes. The first modification would require introducing another pipe from B to A, and the second, *data buffering* in a pipe. Addition of any other components into the system would require further addition and/or replacement of pipes. The penalty we would pay is that these modifications may require substantial system down-time. Pipes can, therefore, accommodate these new requirements, even though constantly adding and replacing them may not be the most effective solution.

If, however, we want to change the nature of the data from an *unformatted byte stream* to *discrete, typed packets* that can be processed more efficiently by the interacting components, pipes will not suffice. In such a case, an *event bus* connector will be a more suitable alternative. Although clearly different types of connectors, pipes and event buses exhibit a number of similar properties, such as loose component coupling, *asynchronous communication*, and possible *data buffering*. At the same time, event buses are better suited to support system adaptation: an event bus connector is capable of establishing *ducts* between interacting components “on the fly;” its *cardinality* is a single *event sender* (similarly to the pipe), but multiple *observers*. Thus, in principle, event buses allow components to be added or removed, and to *subscribe* to *receive* certain events, at any time during a system’s execution. Figure 5-2 abstractly depicts using an event bus to accommodate the above changes.

**Figure 5-2.** An event-based architecture consisting of two components, A and B, communicating via typed discrete data packets (i.e., events) through the event bus connector E. The connector allows “on the fly” system modifications, such as adding a new component C.



## 5.2 Connector Foundations

The underlying, elementary building blocks of every connector are the primitives for managing the *flow of control* (that is, changing the processor program counter) and *flow of data* (that is, performing memory access) in a system. These primitives give enough conceptual power to build sophisticated and complex connectors. In addition to these primitives, every connector maintains one or more *channels*, also referred to as *ducts*, which are used to link the interacting components and support the flow of data and control between them. A duct is necessary for realizing a connector, but by itself, it does not provide any additional interaction services. Very simple connectors, such as module linkers, provide their service simply by forming ducts between components. Other connectors augment ducts with some combination of data and control flow to provide richer interaction services. Very complex connectors can also have an internal architecture that includes computation and information storage. For example, a load balancing connector would execute an algorithm for switching incoming traffic among a set of components based on the knowledge about the current and past load state of components.

Simple connectors are typically implemented in programming languages. On the other hand, composite connectors are achieved through composition of several connectors (and possibly components), and are usually provided as libraries and frameworks. Simple connectors only provide one type of interaction service, whereas composite connectors may combine many kinds of interactions. Complex connectors can help overcome the limitations of modern programming languages. However, when creating such connectors it is important to be able to reason about their underlying, low-level interaction mechanisms, identify the appropriate design choices, and detect potential mismatches among the interaction mechanisms used to compose a connector.

To this end, we will use the connector classification framework shown in Figure 5-3: each connector is identified by its primary service category and further refined based on the choices made to realize these services. The characteristics most commonly observed among connectors are positioned towards the top of the framework, whereas the variations are located in the lower layers. The framework comprises service categories, connector types, dimensions (and possibly their subdimensions), and values for the dimensions. A *service category* represents the broad interaction *role* the connector fulfills. Connector *types* discriminate among connectors based on the way in which the interaction services are realized. The architecturally relevant details of each connector type are captured through *dimensions*, and, possibly, further subdimensions. Finally, the lowest layer in the framework is formed by the set of *values* a dimension (or subdimension) can take. Note that a particular connector instance (that is, *species*) can take a number of values from different types. In other words, this classification does not result in a strict hierarchy, but rather in a directed acyclic graph.

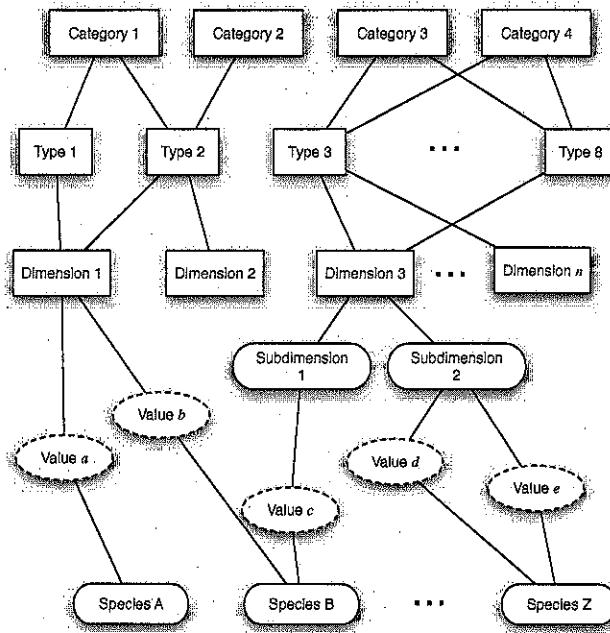


Figure 5-3. A framework for studying software connectors.

The remainder of this chapter describes in more detail the classification framework and a comprehensive taxonomy that can be used as the foundation for studying, classifying, and using software connectors.

### 5.3 Connector Roles

A software connector can provide one or more of four general classes of services:

- communication,
- coordination,
- conversion, and
- facilitation.

Put another way, a connector can play one or more of these four roles. Since these services, or roles, fully describe the range of possible software component interactions, the topmost layer in our classification framework from Figure 5-3 is the service category. We will define and discuss the four service classes, and provide simple examples of each.

#### Communication

Connectors providing communication services support *transmission of data* among components. Data transfer services are a primary building block of component interaction. Components routinely pass messages, exchange data to be processed, and communicate results of computations.

#### Coordination

Connectors providing coordination services support *transfer of control* among components. Components interact by passing the thread of execution to each other. Function calls and method invocations are examples of coordination connectors. Higher-order connectors, such as signals and load balancing connectors, provide richer, more complex interactions built around coordination services.

#### Conversion

Connectors providing conversion services transform the interaction required by one component to that provided by another. Enabling heterogeneous components to interact with each other is a non-trivial task. Interaction mismatches are a major hindrance in composing large systems. The mismatches are caused by incompatible assumptions made by components about the type, number, frequency, and order of interactions in which they are to engage with other components. Conversion services allow components that have not been specifically tailored for each other to establish and conduct interactions. Conversion of data formats and wrappers for legacy components are examples of connectors providing this interaction service.

### Facilitation

Connectors providing facilitation services mediate and streamline component interaction. Even when heterogeneous components have been designed to interoperate with each other, there may be a need to provide mechanisms for further facilitating and optimizing their interactions. Mechanisms such as load balancing, scheduling services, and concurrency control may be required to meet certain non-functional system requirements and to reduce interdependencies among interacting components.

Every connector provides services that belong to at least one of these four categories. Commonly though, connectors provide multiple services in order to satisfy the need for a richer set of interaction capabilities. For example, procedure call, one of the most widely used software connector types, provides both communication and coordination services.

## 5.4 Connector Types and their Variation Dimensions

Interaction services broadly categorizes connectors, but leaves many details unexplained. This level of abstraction cannot help us build new connectors, nor can it be used to model and analyze them in an architecture. Hence, we further classify connectors into eight different types based on the way in which they realize interaction services:

- procedure call,
- event,
- data access,
- linkage,
- stream,
- arbitrator,
- adaptor, and
- distributor.

Connector types are the level at which architects typically consider interactions when modeling systems.

Simple connectors can be modeled at the level of connector types; their details can often be left to low-level design and implementation. On the other hand, more complex connectors often require that many of their details be decided at the architectural level so that the impact of these decisions can be studied early and on a system-wide scale. Those details represent variations in connector instances and are treated as connector dimensions in the below classification. In turn, each dimension has a set of possible values. The selection of a single value from each dimension results in a concrete connector species. Instantiating dimensions of a single connector type forms simple connectors; on the other hand, using dimensions from different connector types leads to a composite (“higher-order”) connector species.

The remainder of this section will describe the key characteristics of each connector type as well as their variation points. Additionally, we will highlight the interaction role(s) played by each connector type. The discussion draws extensively from the connector taxonomy set forth by Mehta, Medvidovic, and Phadke [191]. It should be noted that the characteristics of different connectors discussed below are meant to cover the entire space of connectors; it is possible that an individual connector of a given may not possess a particular dimension.

### 5.4.1 Procedure Call

Procedure call connectors model the flow of control among components through various invocation techniques. They are thus *coordination* connectors. Additionally, procedure calls perform transfer of data among the interacting components through the use of parameters and return values. They are thus also *communication* connectors. These connectors are among the most widely used and best understood connectors, and have been likened to the “assembly language” of software interaction. Examples of procedure call connectors include object-oriented methods; `fork` and `exec` in Unix-like environments, call back invocation in event-based systems, and operating system calls. Procedure calls are frequently used as the basis for composite connectors, such as remote procedure calls or RPC, which also perform *facilitation* services.

The full space of options available to a software engineer for constructing procedure call connectors is shown in Figure 5-4. Note that the values for certain dimensions and subdimensions are not shown: *Multiple* versus *Single Entry Point*, as well as *Fan In* and *Fan Out Cardinality*. These are numerical subdimensions that either take an obvious value (1 in the case of *Single Entry Point*) or can take many values (in the case of the remaining three subdimensions). They are hence elided for simplicity. We will likewise omit the values of all such dimensions and subdimensions in the case of the other seven connector types.

A typical programming language-level procedure call connector takes on a specific set of values from the choices depicted in the figure. For example, as most Java users will readily know, a procedure (that is, method) call provides the *Data Transfer* of its *Parameters* by *Reference*; it may have a *Return value* unless the invoked method is declared as a `void`; it will have a *Single Entry Point*, at the start of the invoked method; it will be a result of *Explicit Invocation*; its *Synchronicity* will be *Blocking*; its *Fan in* and *Fan out Cardinality* will both be 1 – that is, a Java *Method Call* always has a single source and a single destination; finally, its *Accessibility* may be *Public* or *Private*.

At this point, the reader is not necessarily expected to understand all of this connector type's various dimension, subdimensions, and values. Similarly so with the variation points of the remaining seven connector types discussed below and depicted in Figure 5-5 through Figure 5-11. One objective of this chapter is to sensitize the reader to the richness and potential complexity of the space of software connectors.

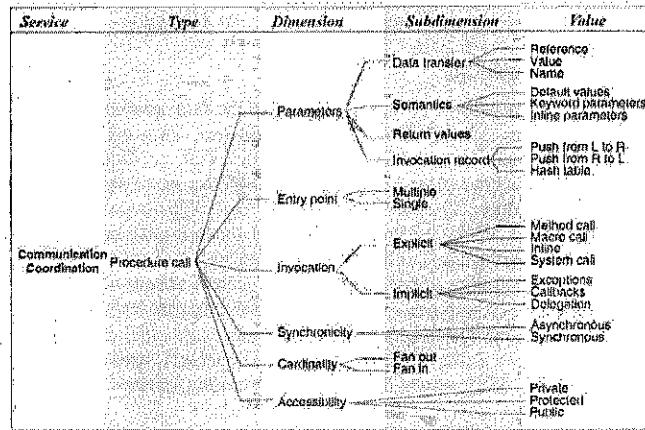


Figure 5-4. Procedure call connector type and its variations.

#### 5.4.2 Event

Rosenblum and Wolf define an event as the instantaneous effect of the (normal or abnormal) termination of the invocation of an operation on an object, which occurs at that object's location. Event connectors are similar to procedure call connectors in that they affect the flow of control among components, and thus provide *coordination* services. In this case, the flow is precipitated by an event. Once the event connector learns about the occurrence of an event, it generates messages (that is, event notifications) for all interested parties and yields control to the components for processing these messages. Messages can be generated upon the occurrence of a single event or a specific pattern of events. The contents of an event can be structured to contain more information about the event, such as the time and place of occurrence, and other application-specific data. Event connectors therefore also provide *communication* services.

Event connectors are also different from procedure calls in that *virtual* connectors are formed between components interested in the same event topics, and those connectors may appear and disappear dynamically.

The full space of options available to a software engineer for constructing event connectors is shown in Figure 5-5. For example, the *Cardinality* of a multicasting event connector (recall the discussion of the C2 architectural style in Chapter 4) will be a single *Producer* and multiple *Observer* components; ideally the connector will support *Delivery* of data *Exactly Once* (whatever is sent by the source component is delivered to the recipient components); its *Synchronicity* may be *Asynchronous* (that is, non-blocking); it could use the *Publish/Subscribe Notification* mechanism; and so on.

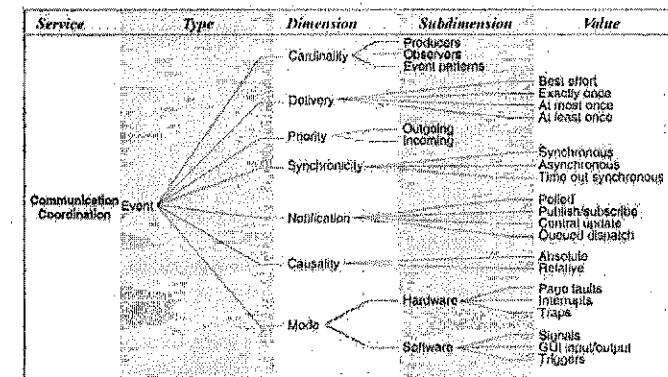


Figure 5-5. Event connector type and its variations.

#### 5.4.3 Data Access

Data access connectors allow components to access data maintained by a data store component. Therefore, they provide *communication* services. Data access often requires preparation of the data store before and cleanup after access has been completed. In case there is a difference in the format of the required data and the format in which data is stored and

provided, data access connectors may perform translation of the information being accessed, that is, *conversion*. The data can be stored either persistently or temporarily, in which case the data access mechanisms will vary. Examples of persistent data access include query mechanisms, such as SQL for database access, and accessing information in repositories, such as a software component repository. Examples of transient data access includes heap and stack memory access, and information caching.

The full space of options available to a software engineer for constructing data access connectors is shown in Figure 5-6. A data access connector could enable *Global* access; allow *Mutating* (that is, changing) the data; it could provide *Persistent* access through *File I/O*; its *Cardinality* would typically be a single entity that *Defines* the data, but multiple entities that *Use* the data; and so on.

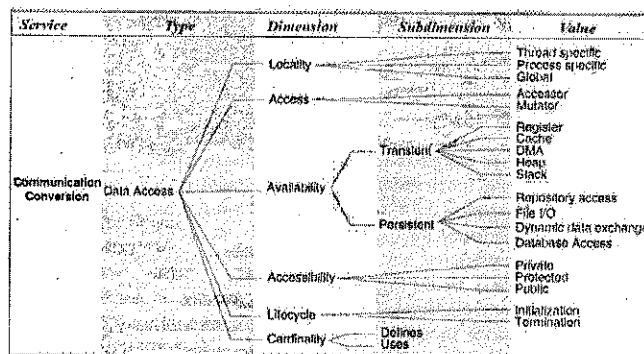


Figure 5-6. Data access connector type and its variations.

#### 5.4.4 Linkage

Linkage connectors are used to tie the system components together and hold them in such a state during their operation. Linkage connectors enable the establishment of ducts, that is, the channels for communication and coordination, which are then used by higher-order connectors to enforce interaction semantics. In other words, linkage connectors provide *facilitation* services.

Once ducts are established, a linkage connector may disappear from the system or remain in place to assist in the system's evolution. Examples of linkage connectors are the links between components and buses in a C2-style architecture (recall Chapter 4) and dependency relationships among

software modules described by module interconnection languages (MIL) [58].

The full space of options available to a software engineer for constructing linkage connectors is shown in Figure 5-7. Compared to the preceding dimensions, this is not a particularly rich connector dimension. The *Reference* to linked components can be *Implicit*, possibly even parameterized and mutable, or *Explicit*. The *Granularity* dimension refers to the size of components and level of detail required to establish a linkage. The subdimensions of *Granularity* (*Unit*, *Syntactic*, and *Semantic*) were directly influenced by Perry's foundational study of software interconnection models [220]:

- *Unit* interconnection specifies only that one component—which can be a module, an object, or a file—depends on another. Examples of unit interconnection are configuration management and system building facilities such as *Make*.
- *Syntactic* interconnection refines this relationship and establishes links between *Variables*, *Procedures*, *Functions*, *Constants*, and *Types* within the linked components. This information can be used in static analysis (e.g., locating unreachable code within a module) and smart compilation, where only the changed portions of a system are recompiled.
- *Semantic* interconnection specifies *how* the linked components are supposed to interact. Semantic interconnection ensures that the interaction requirements and constraints are explicitly stated and satisfied. This typically takes the form of an interaction protocol, such as those discussed in the context of architectural modeling and analysis in Chapter 6 and Chapter 8 respectively.

The *Cardinality* of a linkage connector refers to the number of places in which a system resource—such as a component, procedure, or variable—is *Defined*, *Used*, *Provided*, or *Required*. Typically, a resource is defined and/or provided in a single location and used or required from multiple locations. Finally, a linkage connector can establish the *Binding* between components very early (i.e., prior to system compilation), early (i.e., during compilation), or late (i.e., during the system's execution).

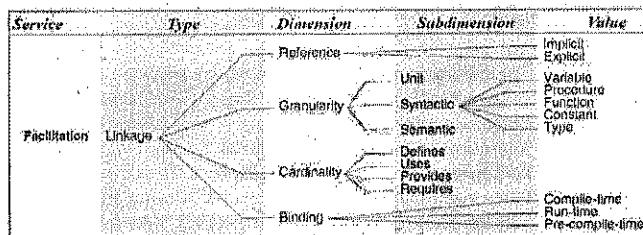


Figure 5-7. Linkage connector type and its variations.

#### 5.4.5 Stream

Streams are used to perform transfers of large amounts of data between autonomous processes. Stream connectors therefore provide communication services in a system. Streams are also used in client-server systems with data transfer protocols to deliver results of computation.

Streams can be combined with other connector types, such as data access connectors, to provide composite connectors for performing database and file storage access, and event connectors, to multiplex the delivery of a large number of events. Examples of stream connectors are UNIX pipes, TCP/UDP communication sockets, and proprietary client-server protocols.

The full space of options available to a software engineer for constructing stream connectors is shown in Figure 5-8. For example, a stream-based connector may be *Unnamed*, as in Unix pipes; it may provide *Synchronous*, *Remote* interaction via *Structured* data; it may guarantee *At least once Delivery*; its *Cardinality* may be *Binary*, i.e., a single *Sender* and a single *Receiver*; finally, its *State* value could be determined by a *Bounded Buffer*.

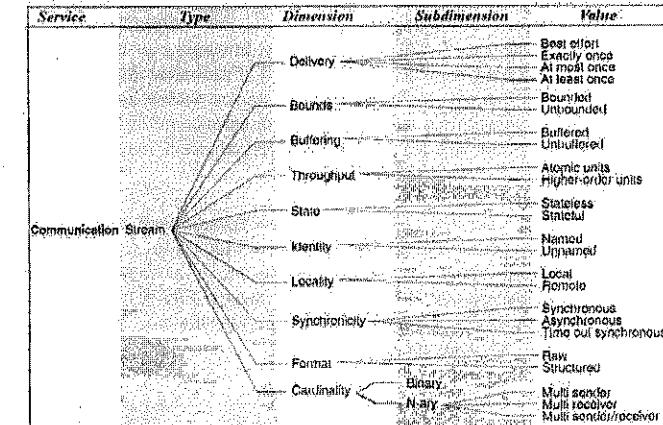


Figure 5-8. Stream connector type and its variations.

#### 5.4.6 Arbitrator

When components are aware of the presence of other components but cannot make assumptions about their needs and state, arbitrators streamline system operation and resolve any conflicts (thereby providing *facilitation* services), and redirect the flow of control (providing *coordination* services). For example, multi-threaded systems that require shared memory access use synchronization and concurrency control to guarantee consistency and atomicity of operations. Arbitrators can also provide facilities to negotiate service levels and mediate interactions requiring guarantees for reliability and atomicity. They also provide scheduling and load balancing services. Arbitrators can ensure system trustworthiness by providing crucial support for dependability in the form of reliability, safety, and security.

The full space of options available to a software engineer for constructing arbitrator connectors is shown in Figure 5-9. Arbitrator connectors can aid with system *Fault handling*, by determining and trapping component faults before they propagate. They can also ensure the appropriate *Concurrency* semantics among the interacting components. For example, arbitrators can employ *Mechanisms*, such as *Semaphores* or *Monitors*, to control access to the interacting components' resources. Arbitrator connectors may also support *Transactions* and guarantee different levels of *Security* (see Chapter 13). Finally, they can control the interacting components' execution *Scheduling*. A specific example of arbitrator connectors is discussed in Section 5.5.

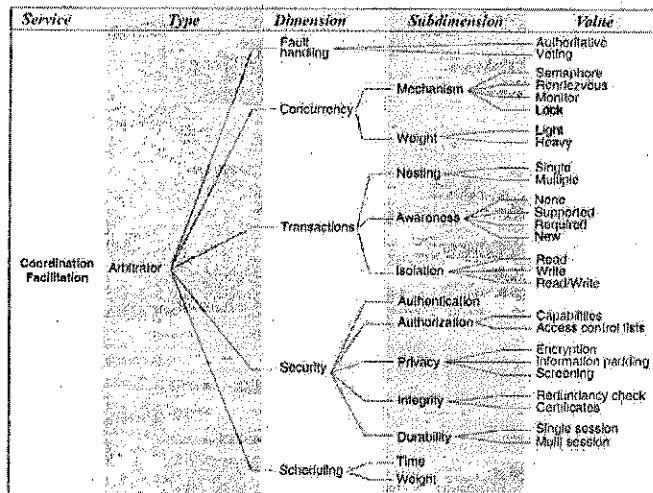


Figure 5-9. Arbitrator connector type and its variations.

#### 5.4.7 Adaptor

Adaptor connectors provide facilities to support interaction between components that have not been designed to interoperate. Adaptors involve matching communication policies and interaction protocols among components, thereby providing *conversion* services. These connectors are necessary for interoperation of components in heterogeneous environments, such as different programming languages or computing platforms. Conversion can also be performed to optimize component interactions for a given execution environment. For example, a distributed system may rely on remote procedure calls (RPC) for all interactions across process boundaries; if two interacting components are collocated within the same process for a given time period, a remote procedure call may be seamlessly converted to a local procedure call during that time. Adaptors may also employ transformations (e.g., table look-ups) to match required services to the available facilities.

The full space of options available to a software engineer for constructing adaptor connectors is shown in Figure 5-10. Examples of adaptors include virtual memory translation; Yellin and Strom's adaptors [306], which match incompatible component interaction protocols; virtual function tables used for dynamic dispatch of polymorphic method calls; and DeLine's packagers, which separate a component's internal functionality,

referred to as *essence*, from the manner in which it is accessed [57]. XML metadata interchange (XMI) is a relatively recent approach that supports interchange of models between applications and performs data presentation conversion.

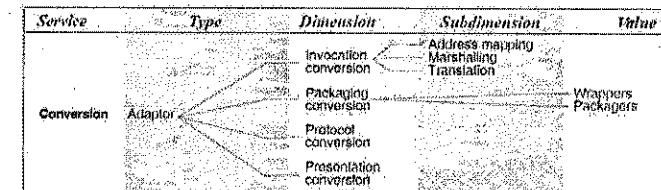


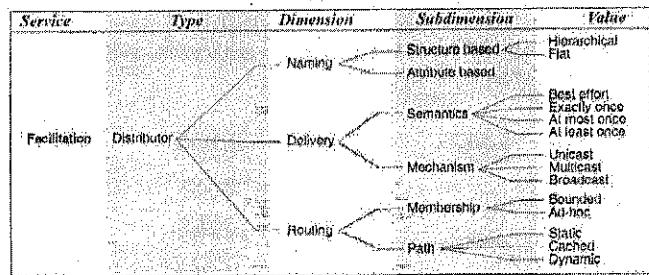
Figure 5-10. Adaptor connector type and its variations.

#### 5.4.8 Distributor

Distributor connectors perform the identification of interaction paths and subsequent routing of communication and coordination information among components along these paths. Therefore, they provide *facilitation* services. Distributor connectors never exist by themselves, but provide assistance to other connectors, such as streams or procedure calls. Distributed systems exchange information using distributor connectors to direct the data flow. Distributed systems require identification of component locations and paths to them based on symbolic names. Domain name service (DNS), routing, switching, and many other network services belong to this connector type. Distributors have an important effect on system scalability and survivability.

The full space of options available to a software engineer for constructing distributor connectors is shown in Figure 5-11. Issues that are particularly important in distributed systems are resource *Naming*; *Semantics* and *Mechanisms* of data *Delivery*; and characteristics of *Routing*.

Figure 5-11. Distributor connector type and its variations.



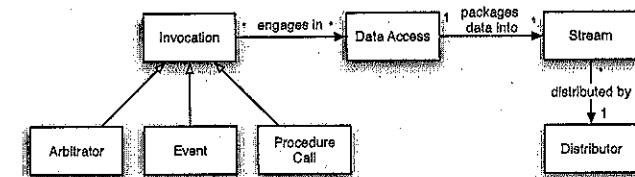
## 5.5 Example Connectors

The reader should be familiar at least with the frequently used procedure call and shared data connector types. It likely that the reader has seen or used several of the other connector types, such as distributors or adaptors, and has also been exposed to composite connectors. Furthermore, Chapter 4 introduced a number of connectors in the different Lunar Lander examples.

In this section, we will illustrate the connector classification discussed above with four composite *distribution* connectors that are in wide use today: event-based, grid-based, client-server-based, and peer-to-peer-based (or P2P-based) connectors. These connectors distribute large amounts of content over a wide area network, such as the Internet. Such connectors are used in disseminating music, movies, scientific data, and so on. Several implementations of these connectors are in wide use by a number of research, industry, and government projects, as well as a large number of individuals around the world.

Distribution connectors can be described as different combinations of the connector types defined in the classification of Section 5.4. The exact combination of the six dimensions varies across the different distribution connectors, but in general, each distribution connector performs some form of *Data Access*, involving a *Stream-based* reading (and packaging) of data, and *Distribution* of the data to end users. Some connector classes are invoked via *Procedure calls* (e.g., client/server-based) while others are invoked via *Events* (e.g., Event-based), or *Arbitration* (e.g., P2P-based). Figure 5-12 illustrates the choices and the relationships.

Figure 5-12. Data distribution connectors involve a type of invocation (via arbitrator, event, or procedure call connectors), data access, stream, and distribution. Cardinality is indicated accordingly on the relationship arrows, where \* refers to the cardinality of "many".



The remainder of this section describes each of the four data distribution connectors using the connector classification from Section 5.4. The seemingly verbose description of the connectors is necessary: it reflects the number of concerns an architect has to consider when selecting and composing connectors for a specific system, as well as the number of decisions that will be made in the process.

### 5.5.1 Event-based Data Distribution Connectors

The event-based data distribution connectors are compositions of four of the connector types from Section 5.4: event, data access, stream, and distributor.

The event-based data distribution connectors send and receive data through asynchronous notifications called *events*. Events may arrive according to some fixed periodic schedule or at discrete aperiodic intervals. Typically there are many producers and consumers of data in event-based distribution connectors. For example, science data servers (producers) may alert scientists (consumers) of the availability of new data sets. Event-based distribution connectors often employ an asynchronous best-effort delivery method for data, making no guarantees as to the completion or time of data deliveries. Data delivery events sent through the connectors can be prioritized, tailored to different use cases or deployment environments, and specified by system users. Events can be delivered using prioritized threaded queues, be locally or remotely managed, or delivered using user registered preferences and the publish-subscribe delivery mechanism.

Event-based distribution connectors can *access* and *mutate* data at both the producer and the consumer end. Event-based distribution connectors themselves access transient and persistent data, both public and private. They communicate with transient session-based stores such as shared

memory stores (e.g., Apache's Derby [11]). They also communicate with persistent stores such as repositories, databases, file systems, and Web pages.

After data access by event-based distribution connectors, data is typically packaged into *streams*, both structured and raw, using a best effort approach, with bounded packet size and data buffering. Streams can be identified via named uniform resource identifiers (URIs), and constructed using the asynchronous mode of operation. Streams may be constructed either locally or remotely, depending upon how the data was accessed.

Stream based data is *distributed* from data producers to data consumers using a naming registry, via either a hierarchical or flat-based naming model. Data streams are delivered as events using best effort delivery, and any combination of the unicast, broadcast, or multicast delivery mechanisms. Routing of events is typically determined by the specific network layer of the connector's deployment environment.

Example instances of event-based data distribution connectors include the Siena publish-subscribe middleware [36], the Prism-MW middleware [180] and its subsequent extensions allowing grid resource location and discovery called GLIDE [184].

### 5.5.2 Grid-based Data Distribution Connectors

The grid-based data distribution connectors are compositions of four of the connector types from Section 5.4: procedure call, data access, stream, and distributor.

The grid-based family of distribution connectors moves and delivers large amounts of data between software components deployed in the *grid* environment: a virtual network of shared computing and data resources. Although the grid is further discussed in Chapter 11, this section will outline the architecture of the corresponding connectors. The reader may find it useful to return to this section again after reading Chapter 11.

Grid-based distribution connectors are invoked via a named, synchronous *procedure call*, often as a web service call sent using SOAP [194]. User authentication credentials are provided to the connector for integration with the Grid Security Infrastructure (GSI), a highly secure toolkit based on keypairs and certificate authorities. URLs sent via the connector invocation describe where the data is, and where it is to be sent (that is, who the consumers are). Parameters are passed by value using "keyword equals value" semantics, with control messages being logged to the Grid API log layer.

Grid-based distribution connectors *access* and *mutate* transient and persistent data, both private and public, as long as there is some type of standard API (e.g., dynamic data exchange over XML, a repository access, or file I/O) for accessing it.

Data access through a grid connector is typically packaged as a *stream* of bytes (or blocks, configured via a parameter) with exactly-once delivery, and (configurable) bounded buffering provided by the network's TCP/IP level. Data can be structured or raw. Buffering and throughput of data are parallelized via multiple concurrent time-out synchronous TCP/IP streams. Streams are named stateful URLs and URIs, and can exist both locally and remotely, depending upon where the data was accessed. A stream can be delivered to many consumers.

Grid-based distribution connectors *distribute* data using the grid environment for naming and location, including the Grid Metadata Catalog Service (MCS) and Replica Location Service (RLS) components, and named URLs and URIs. Naming can be hierarchical, with resources and locations sharing parent-child relationships via the MCS. Alternatively, naming and discovery can be flat, structure-based. Data is delivered via parallelized unicast exactly once using TCP/IP concurrent streams, flooding the underlying network to its saturation, thus making the most efficient use of the available bandwidth possible. Reliability measures allow redelivery of lost packets if necessary as well as partial data transfers, both sequential and out of order. Routing of data is handled by the underlying TCP/IP network layer.

Example instances of grid-based distribution connectors include the GridFTP software, bundled along with the Globus Grid Toolkit [280], and the large files transfer protocol, or bbFTP [71].

### 5.5.3 Client-Server-based Data Distribution Connectors

The client-server-based distribution connectors allow seamless distribution of data between distributed systems using RPC. These connectors are compositions of four of the connector types from Section 5.4: procedure call, data access, stream, and distributor.

Client/server-based distribution connectors are invoked via a synchronous remote *procedure call* that appears (to the consumers of data) as if it were a local method call. Keyword (named) parameters are passed to the method call to specify the distribution constraints, with parameters being passed by value or reference, depending upon the underlying remote procedure call implementation. Methods can have return values, which typically must conform to a standard set of primitive data types that are supported on all machines involved in the data distribution. Methods are

interactions between one sender and one receiver, typically the producer of the data and its consumer, respectively.

Upon invocation, the client/server-based distribution connector engages in a *data access*, accessing and mutating persistent and transient data.

After data is accessed, it is packaged into *streams* that are delivered using exactly-once delivery and bounded packet size managed by the underlying TCP/IP protocol. Data can be raw or structured in the stream. Stream throughput is measured in atomic units (bits per second), and streams are identified using stateful, named URNs. Streams can be local or remote, depending on where the data was accessed or packaged.

Data is *distributed* from client-server-based connectors using a naming registry to locate the requesting consumer of data. Data is delivered through method (or interface) parameters and return values. It is sent exactly once, using the unicast delivery mechanism. Routing is performed by the underlying TCP/IP network using static membership identified via a naming registry.

Example instances of client-server-based data distribution connectors include HTTP/REST (recall Chapter 1), Java RMI, CORBA (recall Chapter 4), FTP, SOAP, and many commercial UDP technologies.

#### 5.5.4 P2P-based Data Distribution Connectors

The P2P-based data distribution connectors are compositions of four of the connector types from Section 5.4: arbitrator, data access, stream, and distributor.

The P2P-based distribution connectors are unlike the other three categories. Rather than providing some sort of initial procedural or event-based invocation, these connectors typically rely on *arbitration* as a means of synchronization and invocation. Arbitration involves control flow redirection between distributed resources, or peers, operating in a networked environment. Arbitrators can negotiate protocols and scheduling and timing issues. Fault handling and parameter passing is handled in an egalitarian fashion via voting and point-to-point or point-to-many communication between peers or groups of peers. P2P-based distribution connectors use rendezvous as a mechanism to achieve concurrency and scheduling. Transaction support is often available, and invocation can be rolled back if necessary.

Upon invocation, peers in a P2P-based distribution connector engage in *data access*, accessing transient (both process- and thread-specific) and persistent (e.g., repository, file I/O, and so on) data. Since peers can come

and go in a P2P-based scenario, for the most part data access is transient in nature: a peer need not stick around for the entire distribution.

Data is accessed and packaged via *streams*, using a best effort bounded mechanism. Data can be structured or raw, as long as it can be organized into identifiable chunks that can be retransmitted and shared between peers handled by the connector. Streams are named URNs typically identified using some hashing algorithm (e.g., SHA-1 or MD5), and are available both locally and remotely depending upon where the data was accessed or packaged.

Data is *distributed* in the P2P-based distribution connectors by locating other peers that have pieces of data a user would like to obtain or distribute. Location of other peers is based upon attributes such as resource type, SHA-1, and other domain-specific attribute metadata (e.g., for movie files “production company” might be used, or for music “artist name”). Delivery occurs in the form of chunks, sent to and from other peers using best effort or at least once semantics over unicast and multicast transmission channels. Routing, while influenced by the underlying network layer, is handled by some sort of tracking mechanism, sometimes called trackers or super peers. Tracking mechanisms allow location of chunks of data streams that need to be distributed or obtained in a P2P-based connector.

Example instances of the P2P-based distribution connector class include BitTorrent [43] and JXTA-based data distributors, such as the Peerdata project at NASA’s Jet Propulsion Laboratory. P2P systems employing such connectors are discussed in Chapter 11.

### 5.6 Using the Connector Framework

This section provides general guidelines for software architects in selecting connectors that meet their needs. The section discusses the issue of connector compatibility: understanding which connectors, or connector dimensions, are compatible and which ones are not is particularly important in cases where composite connectors are needed.

#### 5.6.1 Selecting Appropriate Connectors

In selecting a software connector that meets the particular needs of a given (sub)system, a software architect must perform at least the following steps. Note that the descriptions of the steps are relatively general, meaning that this process places significant responsibility on the software architects and requires a great deal of familiarity with the technical details of connectors that are at their disposal.

1. Select the specific set of interacting components. Different sets of components, even in the same system, may have different interaction needs. This is why it is important for the architect to focus only on those components for which the desired connector is needed. This and the subsequent steps are repeated for each such component set, that is, for as many distinct connectors as are needed in the system.
2. Determine the interaction services the components need. It is critical to identify the precise characteristics of the components' interaction. This will likely involve studying the components' architectural descriptions, and may also require considering the implementation language and/or framework.
3. Based on the identified interaction services, determine a subset of the eight connector types that comprise the initial candidate set for providing those services. It is sufficient to establish that the connector types chosen in this step *may* be a good candidate for supplying the needed services.
4. Evaluate each connector type from the chosen subset based on the details of the interaction requirements. Study these in light of the connector types' dimensions, subdimensions, and values. Eliminate any connector types whose usage is deemed to result in a suboptimal interaction solution for the specific set of components under consideration.
5. For each of the remaining candidate connector types, set the values for the necessary dimensions and subdimension as appropriate. Identify the best ("most natural") candidate connectors. This will require performing a trade-off analysis among multiple possible solutions. It may also result in selecting a composite connector, which combines features of multiple types, as further discussed below.

The classification of connectors described in Section 5.4 thus serves as the foundation for synthesizing new connectors as well as analyzing the compatibility of connector dimensions. Instantiating dimensions of a single connector type by choosing one or more values forms a simple connector species; on the other hand, using values of dimensions from different connector types leads to a composite ("higher order") connector species. Many real-world scenarios force an architect to compose such higher-order connectors to satisfy all application requirements.

The reader should note that creating unprecedented, composite connectors is not a trivial task. At the least, this requires developing a deep

understanding of the connectors' complementary, orthogonal, and incompatible characteristics. Without such an understanding, the resulting integration process may be misguided and the developed solutions suboptimal, or worse, completely ineffective. Examples of this have been documented in the literature (e.g., in the well known case of the interactions among the large components used in the Aesop system [88]).

In the absence of a set of concrete, well understood, and widely adopted rules for defining composite connectors, it becomes difficult to guide this process. Recent research by, for example, Spitznagel and Garlan [263] suggests some specific formalisms and strategies that can be adopted to address connector composition. However, ultimately a comprehensive classification of connectors, such as the one presented in this chapter, is necessary (though not sufficient) to create a general set of guidelines that specify the condition under which two or more connectors can be composed. We discuss this issue in more depth next.

### 5.6.2 Detecting Mismatches

The connector taxonomy introduced in Section 5.4 can be leveraged to identify potential mismatches between incompatible connector dimensions, and to avoid such combinations. Figure 5-13 shows a compatibility matrix for the connector dimensions identified in the classification from Figure 5-4 through Figure 5-11, and provides guidance for which combinations are necessary for using a connector and which ones should be avoided. The sparseness of the matrix suggests that the allowed design space of connectors appears to be very large based on their current understanding, but some pitfalls are known to exist and should be avoided.

	Procedure call	Event	Stream	Data access	Object	Document	Arbitrator	Adaptor	Adapter	Delivery
	Dimensions	Procedure call	Event	Data access	Object	Document	Arbitrator	Adaptor	Adapter	Delivery
Procedure call	Dimensions	Procedure call	Event	Data access	Object	Document	Arbitrator	Adaptor	Adapter	Delivery
Dimensions	Procedure call	Event	Data access	Object	Document	Arbitrator	Adaptor	Adapter	Delivery	
Procedure call	Procedure call	Event	Data access	Object	Document	Arbitrator	Adaptor	Adapter	Delivery	
Event	Procedure call	Event	Event	Data access	Object	Document	Arbitrator	Adaptor	Adapter	Delivery
Data access	Procedure call	Event	Event	Data access	Object	Document	Arbitrator	Adaptor	Adapter	Delivery
Object	Procedure call	Event	Event	Data access	Object	Object	Arbitrator	Adaptor	Adapter	Delivery
Document	Procedure call	Event	Event	Data access	Object	Object	Arbitrator	Adaptor	Adapter	Delivery
Arbitrator	Procedure call	Event	Event	Data access	Object	Object	Arbitrator	Adaptor	Adaptor	Delivery
Adaptor	Procedure call	Event	Event	Data access	Object	Object	Arbitrator	Adaptor	Adaptor	Delivery
Adapter	Procedure call	Event	Event	Data access	Object	Object	Adaptor	Adaptor	Adaptor	Delivery
Delivery	Procedure call	Event	Event	Data access	Object	Object	Adaptor	Adaptor	Adaptor	Delivery

Symbol	Rule	Modality	Meaning
&	Cautions	Mandatory	The two dimensions are required simultaneously, but have restrictions on certain combinations.
☒	Prohibits	Optional	The combined use of the two dimensions is disallowed.
◎	Restricts	Optional	The combined use of the two dimensions has restrictions.
&	Requires	Mandatory	The two dimensions are always required simultaneously.

Figure 5-13. Connector compatibility matrix.

Four kinds of rules for combining connector dimensions can be identified: cautions, requires, restricts and prohibits. The *cautions* rule indicates that certain combinations of values for two connector dimensions, that are required to be used in tandem, may result in an unstable or unreliable connector. For example, a component being invoked implicitly cannot have multiple entry points since an implicit invocation mechanism cannot choose among the entry points.

The *requires* rule indicates that the choice of a dimension requires another dimension to also be selected in a connector species. It also allows all possible combinations of the given dimension and its required co-dimension. This chaining rule is the basis for constructing the base connector species. For example, an event connector that requires delivery semantics also needs a notification dimension, which in turn requires cardinality, synchronicity and mode. This chaining rule results in identification of dimensions that are mandatory in all species of a connector type, and those that are optional. In Figure 5-13, the mandatory dimensions are bold-faced, whereas the optional dimensions are in regular

font. Some dimensions are required only in other connector types and are italicized in the matrix.

The *restricts* rule is used to indicate that the two dimensions are not required to be used together at all times, and that there are certain combinations of their values that are invalid. This rule is used to prevent mismatches similar to the cautions rule. For example, thread-specific data access cannot use heavy-weight concurrency (see the intersection of *Data access - Locality* with *Arbitrator - Concurrency*). On the other hand, the cautions rule mandates the use of a co-dimension even though some combinations of the values of the two dimensions are invalid.

Finally, the *prohibits* rule is used to exclude any combination of two dimensions from being used and indicates total incompatibility of the dimensions. For example, stream delivery cannot be built on transactional atomicity (see the intersection of *Stream - Delivery* with *Arbitrator - Transactions*).

While Figure 5-13 illustrates the constraints on the binary combinations of connector dimensions, the compatibility relations between dimensions are transitive. In other words, the compatibility rules can be successively applied to determine the n-ary compatibility between dimensions. The binary relations outlined in this section would serve as a necessary starting point for analyzing the n-ary relations.

Explicit, targeted study of software connectors is a relatively recent occurrence. There are still many details that need to be uncovered and understandings improved. Figure 5-13 is indicative of this: the sparser reflexive sections of the compatibility matrix (that is, those that combine the dimensions of a single connector type) argue for the need for greater understanding of the given connector type (e.g., arbitrator and adaptor). On the other hand, the dimensions of a connector type with rich constraints indicate greater degrees of understanding and consensus (e.g., procedure call, event, and linkage).

## 5.7 End Matter

Every software system employs connectors, frequently many of them. In complex distributed systems in particular, connectors can be the key determinants of whether the desired systems properties will be met. This observation is often made, yet connectors are not always given "first class" status in software systems, and have certainly not been studied to the same extent as components.

This chapter has presented a detailed study of software connectors. At the most basic level, each connector establishes a conduit (which can be thought of, and referred to, as a virtual channel or duct) for two or more

components to interact by exchanging control and data in a software system. The actual manner in which data and/or control are exchanged, however, and the specific characteristics of how they are exchanged, can vary widely. This is what makes the space of software connectors quite large and complex.

As this chapter has argued, the space of connectors can be better understood by considering the *role* (or roles) played by a given connector, and the *type* (or types) of interaction supported by the connector. At the same time, the large number of variation points for each connector type (the dimensions, subdimensions, and values introduced in Section 5.4) require that the (in)compatibilities among connectors be considered carefully. While this area clearly requires further study, the existing body of knowledge, if applied judiciously, can be a great aid to software architects and developers.

**The Business Case**

The engineering of complex software systems is difficult and expensive. In particular, composing large components, many of which may not have been developed to "play" together, can cause bloated systems with unacceptable performance, project schedule slippages, and budget overruns. Examples of software projects that fit this general description abound.

If connectors in such scenarios are not considered explicitly, then every pair of components that needs to be integrated may need to be dealt with separately. While past experience may prove useful to architects and developers of such systems, the usually applied techniques (e.g., building wrappers and "glue code") will need to be re-applied in each individual case. Furthermore, this integration code will often be tightly coupled with one or more of the interacting components, rendering its reuse difficult or impossible. Perhaps most importantly, by constantly going back to the same integration "toolbox", software engineers are likely to miss more appropriate, and perhaps less costly, component integration and interaction solutions.

Having an intimate understanding of connectors, and treating them separately from the components, can potentially address all of the above concerns. One useful property of connectors, which is not shared by many components, is that they are largely application-independent. This means that there is actually a finite (although very large) number of component interaction and integration challenges. Many such challenges may be similar across like products (e.g., in a product family) or within a particular application domain.

A given software development organization could thus develop and grow

a large, reusable arsenal of explicit connectors, which would, in turn, help to curb the costs of future projects.

## 5.8 Review Questions

1. Define a software connector.
2. How are connectors different from components?
3. What is a duct? What purpose does it serve?
4. What is the difference between the transfer of control and the transfer of data?
5. Name and describe the four possible roles played by a connector.
6. How is facilitation different from conversion?
7. Name and briefly describe the eight different connector types.
8. Why is connector composition challenging?
9. Are there connector types that can always be composed?
10. Are there types that can never be composed?
11. What are data-intensive connectors?
12. What characteristics do all data-intensive connectors share?

## 5.9 Exercises

1. For each connector type discussed in this chapter, try to identify a specific connector species that belongs to that type.
2. For the connectors identified in the previous question, enumerate the dimension and subdimension values that each of the connector species takes.
3. Analyze the connectors used in the different Lunar Lander examples in Chapter 4 to determine the connector types to which they belong. Specify the values they take for different dimensions and subdimensions.

4. Consider the Aesop system developed by Garlan et al. and described in [88]. Develop a detailed strategy for integrating Aesop's four major components by explicitly treating its connectors. Would your strategy have helped Aesop's developers to deal with the architectural mismatches among the components more effectively than their adopted strategy?
5. Select a software system with which you are intimately familiar. Isolate one of the connectors in the system (e.g., a procedure call connector). Replace that connector with a connector of a different type (e.g., an event connector). What were the required steps in doing so? Discuss the lessons learned.
6. Select a software system with which you are intimately familiar and which uses mostly procedure call connectors. Replace all procedure call connectors in the application with explicit, named connectors, thereby completely decoupling the interacting components. Discuss the relative merits of the two applications' architectures.
7. Repeat the above exercise by changing one or more connectors that support synchronous interaction between components with connectors that support asynchronous interaction. What challenges did you face in accomplishing this task? Does the modified application exhibit the same behavior as the original application? Why or why not?
8. Several open-source systems, available from SourceForge.net and similar online repositories, are accompanied by thorough design documentation. Select at least two open-source systems and study their architectures. Identify their connectors. Classify the connectors according to their types. Can you spot any trends in the systems' connector usage?
9. Mehta et al. [191] have argued that the Linux *Process Scheduler* subsystem identified in the study by Bowman et al. [26] is, in fact, a connector. Investigate the implications of this decision. In order to do so, you may want to consider treating *Process Scheduler* as a component, or as a sub-architecture comprising a composition of finer-grain components and connectors. Were Mehta et al. correct in their decision? Does their decision fundamentally alter the architecture of Linux, or one's understanding of it?
10. This chapter has suggested that, architecturally, the different classes of data-intensive connectors are similar to a certain extent. Select two such widely used connectors from different categories – e.g., client-server and peer-to-peer. Based on their architectures discussed in

- Section 5.5, outline a strategy for converting one connector into the other.
11. Study the previous question's two connectors' architectures and implementations in more detail. Was your conversion strategy viable? If so, proceed with the conversion. If not, discuss the reasons why, adjust your strategy as appropriate, and proceed with the conversion.

## 5.10 Further Reading

Software connectors have been an important facet in developing large, complex software intensive systems for a long time. While they may not have been the primary focus of study, and may not have been identified explicitly, connectors figured prominently in the operating systems, programming languages, distributed systems, computer networks, and middleware literature (e.g., [240], [45], [306], [217]).

The explicit focus on software connectors is more recent and has emerged from the body of work dealing with software architecture. Perry [220] provided the needed foundation in his study of software interconnection models. Perry and Wolf [221] were the first to suggest connectors as first-class entities in a software architecture, and Shaw and Garlan [256] [258, 259] soon followed suit. Allen, Garlan, and Ockerbloom [88] demonstrated that explicit connectors can provide a substantial aid in system specification, and can carry significant, inherent analytical power.

Several researchers have tried to classify connectors as an aid to software architects in making the most appropriate design choices. An early such effort by Hirsch, Uchitel, and Yankelevich [120] was limited in scope, but it directly inspired the more detailed study by Mehta, Medvidovic, and Phadke [191], which has been referenced extensively in this chapter. Bálek and Plášil [13] have proposed a formal connector model for dealing with software deployment (recall Chapter 3). In particular, they posit that the basic set of dynamic services that a connector should provide to aid deployment maps directly to the key service categories in Mehta et al.'s taxonomy: control and data transfer, interface adaptation and data conversion, access coordination and synchronization, communication intercepting, and dynamic component linking. Bálek and Plášil additionally demonstrate that their connectors can be composed to provide more advanced interaction services, in a similar vein to Spitznagel and Garlan's later work [263].

## CHAPTER 6

# 6 Modeling

As we have stated, every software system has an architecture, whether it is a “good” architecture or not. We have previously defined architecture as the set of principal design decisions about a system. Once design decisions have been made, they can be recorded. Design decisions are captured in *models*; the process of creating models is called *modeling*. From Chapter 3 we have:

**Definitions.** An architectural *model* is an artifact that captures some or all of the design decisions that comprise a system’s architecture. Architectural *modeling* is the reification and documentation of those design decisions.

Models can capture architectural design decisions with varying levels of rigor and formality. They enable users to communicate about, visualize, evaluate, and evolve an architecture. Without models, architectures are inscrutable.

Throughout the chapter, we will also discuss how architecture modeling *notations* are used to capture design decisions.

**Definition.** An architectural modeling *notation* is a language or means of capturing design decisions.

As we will discuss, available architecture modeling notations range from the rich and ambiguous (e.g., natural language) to the semantically narrow and highly formal (e.g., the Rapide architecture description language). While some models conform to a single notation, a model may also use a mix of different notations. For example, a single model may use the UML class diagram notation to describe the classes in a system, but annotate them with natural language descriptions of their functions.

This chapter will introduce a broad variety of modeling concepts that are captured in architectural models, from basic architectural elements (e.g., components and connectors) to more complex properties of systems such as behavioral models. It will then cover some of the many available

options for capturing different aspects of an architecture, from the semantically weak (e.g., PowerPoint modeling) to those with formal semantics. Finally, it will discuss the strengths and weaknesses of some of these notations as it applies to some of the systems we’ve discussed already, such as Lunar Lander and the World Wide Web.

### Outline of Chapter 6

- 6 Modeling
  - 6.1 Modeling Concepts
    - 6.1.1 Stakeholder-driven Modeling
    - 6.1.2 Basic Architectural Concepts
    - 6.1.3 Elements of the Architectural Style
    - 6.1.4 Static and Dynamic Aspects
    - 6.1.5 Functional and Non-Functional Aspects
  - 6.2 Ambiguity, Accuracy, and Precision
  - 6.3 Complex Modeling: Mixed Content and Multiple Views
    - 6.3.1 Views and Viewpoints
    - 6.3.2 Consistency among Views
  - 6.4 Evaluating Modeling Techniques
  - 6.5 Specific Modeling Techniques
    - 6.5.1 Generic Techniques
    - 6.5.2 Early Architecture Description Languages
    - 6.5.3 Domain- and Style-Specific ADLs
    - 6.5.4 Extensible ADLs
  - 6.6 When Systems Become Too Complex to Model
  - 6.7 End Matter
  - 6.8 Review Questions
  - 6.9 Exercises
  - 6.10 Further Reading

## 6.1 Modeling Concepts

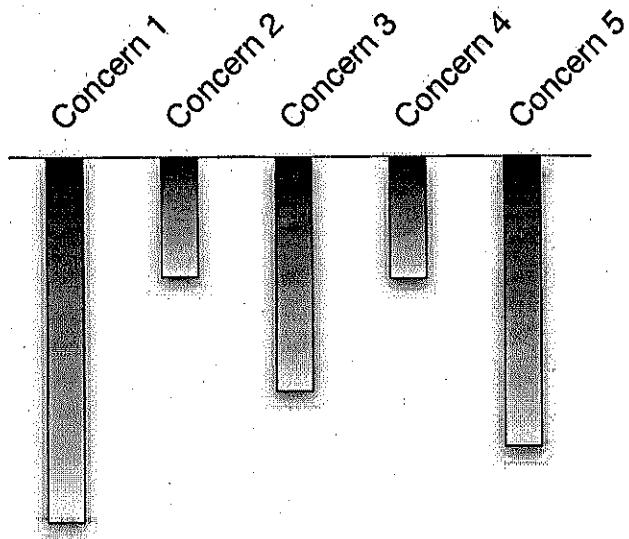
In this chapter, we will discuss a broad spectrum of *kinds* of things that can be modeled in an architecture, and then discuss how various notations can be selected and used to facilitate this modeling. Specifically, for each concept we identify, we will identify what it takes to effectively model that concept—what notational features, and so on.

### 6.1.1 Stakeholder-driven Modeling

One of the most critical decisions that architects and others stakeholders will make in developing an architecture is to choose:

1. What architectural decisions and concepts should be modeled,
2. At what level of detail, and
3. With how much rigor or formality.

These decisions should be made based on *costs* and *benefits*. Architects should balance the benefits of having certain models in certain forms or notations with the costs of creating and maintaining those models. Thus, the choice of what to model, and at what level of detail, will be *stakeholder-driven*. A good rule-of-thumb is that the most important or critical aspects of a system should be the ones that are modeled in the greatest detail with the highest degrees of rigor/formality.



**Figure 6-1.** Modeling different concerns with different depths (from Maier and Rechtin)

Figure 6-1, borrowed from Maier and Rechtin's book *The Art of Systems Architecture* [178], depicts this concept graphically. It shows five concerns about the system identified by stakeholders. In this particular case, Concern 1 is of great importance, and will be considered and modeled deeply—in great detail. Concerns 2 and 4 are less important and are modeled shallowly. Because the concerns and their relative levels of importance will vary from project to project, each project will have somewhat different modeling needs.

Modeling is an activity, and as such it is often governed by a process. It will undoubtedly be part of the larger process of architecture-centric software development that we have been discussing in this book. However, modeling itself is a subprocess, and the process of modeling can vary widely from project to project.

The basic activities behind stakeholder-driven modeling are:

1. Identify relevant aspects of the software to model.
2. Roughly categorize them in terms of importance.
3. Identify the goals of modeling for each aspect (communication, bug finding, quality analysis, generation of other artifacts, and so on).
4. Select modeling notations that will model the selected aspects at appropriate levels of depth to achieve the modeling goals.
5. Create the models.
6. Use the models in a manner consistent with the modeling goals.

Although the steps outlined above are in rough chronological order, it is likely to be more useful to make them part of an iterative process. It is almost never clear from the outset of a project what all the important aspects of a software system are, what the goals of modeling are, and whether those goals are achievable using available notations, technology, time, and money. As such, these estimations must be re-evaluated and refined multiple times through a system's development and the models adjusted accordingly.

### 6.1.2 Basic Architectural Concepts

While every architecture is different, we have previously identified (particularly in Chapter 4) certain kinds of elements that are of importance when talking about architectural designs. These include:

**Components:** Architectural building blocks that encapsulate a subset of the system's functionality and/or data, and restricts access to them via an explicitly defined interface.

**Connectors:** Architectural building blocks tasked with effecting and regulating interactions among components.

**Interfaces:** The points at which components and connectors interact with the outside world—in general, other components and connectors...

**Configurations:** A set of specific associations between the components and connectors of a software system's architecture. Such associations may be captured via graphs whose nodes represent components and connectors, and whose edges represent their interconnectivity.

**Rationale:** Information about why particular architectural decisions were made, and what purpose various elements serve.

These concepts form a starting point for architectural modeling. At the most basic level, modeling these concepts requires a notation that can express a graph of components and connectors, preferably with well-defined connection points (interfaces). These languages can be relatively simple—basic box and arrow diagrams or lists with appropriate internal references will suffice. Rationale is somewhat different because it is more

amorphous. Rationale is primarily used for communicating information and intent between stakeholders, and is generally not codified in the actual, built software system. As such, languages for expressing rationale need to be more expressive and less constrained—rationale is most often expressed using natural language for this reason.

Modeling at only the most basic level (i.e., enumerating the existence and interconnections of the various components and connectors) provides a small amount of value, but these models will not suffice for most complex projects. Rather, these models must be extended and annotated with a host of other concepts: How are the functions partitioned among the components? What are the nature and types of the interfaces? What does it mean for a component and a connector to be linked? How do all these properties of a system change over time? These questions are at the heart of architectural modeling.

Depending on the nature of the system being developed and the domain, it may or may not be straightforward to represent these basic elements. For example, in a desktop application such as a word processor or spreadsheet, the software components and connectors will be relatively static and few in number. Even with a very complex desktop application containing, say, 500-1000 components and connectors, it is feasible to enumerate and describe each of these elements as well as the interconnections among them.

Applications that are large, dynamic, and distributed may be harder to model. For example, it is basically impossible to enumerate all the software components that are part of the World Wide Web or their configuration; there are too many of them and they are constantly coming and going. For these applications, it is probably more reasonable to model only parts of the system, or specific configurations that represent expected use cases. Alternatively, it may be more effective to model the architectural style that governs what kinds of elements may be included in the architecture and how they may be configured.

### 6.1.3 Elements of the Architectural Style

Recall that an architectural style is a set of design decisions that are applied to development in order to elicit desired qualities in the target system. In addition to modeling basic architectural elements, it is often useful to model the style that governs how these elements have been (and may be) used.

Explicitly modeling the architectural style can be helpful for a number of reasons. It reduces confusion about what is and what is not allowed in the architecture. It can help to reduce architectural drift and erosion. It makes it easier to distinguish whether a specific design decision in an architecture

was made to conform to a stylistic constraint, or for some other reason. It can help to guide the evolution of the architecture. It can be more feasible and useful than structural modeling (component and connector graphs) for large or dynamic systems. Because styles are generally applicable to many projects, style models can be reused from project to project. Styles represent a single place to capture cross-cutting concerns and rationale for an architecture.

Some kinds of design decisions that might be captured in a style model include:

**Inclusion of specific elements (e.g., components, connectors, interfaces):** A style may prescribe that particular components, connectors, or interfaces be included in architectures or used in specific situations. This can be facilitated by a modeling approach that supports templates or base models that are then elaborated.

**Component, connector, and interface types:** specific *kinds* of elements may be permitted, required, or prohibited in the architecture. Many modeling approaches are accompanied by a type system, although they often have different semantics.

**Interaction constraints:** constraints on interactions between components and connectors. These constraints can take many forms. They may be temporal ('calling components must call `init()` before any other method'). They may be topological ('only components in the *client* layer are allowed to invoke components in the *server* layer'). They may specify particular interaction protocols, either by name (FTP, HTTP) or specification (formal protocol specifications in a language such as CSP or sequence charts). Modeling approaches that support constraints generally leverage some sort of logic—first order logic, temporal logic, and so on.

**Behavioral constraints:** constraints on the behavior of architectural elements, or kinds of elements. These constraints can run the gamut from simple rules to full-blown complete behavioral specifications for components expressed in a notation like finite state automata. Again here, modeling approaches that support behavioral constraints either use logic or other formal models (automata diagrams).

**Concurrency constraints:** constraints on which elements perform their functions concurrently, and how they synchronize access to shared resources. Approaches that support concurrency modeling often employ formal behavioral models of various architectural elements. Many of them also include temporal modeling techniques such as sequence charts and statecharts.

### 6.1.4 Static and Dynamic Aspects

Many architectures prescribe both static and dynamic aspects of a system. Static aspects are those that do not change as a system runs. Dynamic aspects are affected by the execution of the described system.

Static aspects are generally easier to model simply because they do not involve changes over time. Typical models of static system aspects might include component/connector topologies, assignments of components and connectors to processing elements or hosts, host and network configurations, or mappings of architectural elements to code or binary artifacts.

Dynamic aspects of a system can be harder to model because they must deal with changes to a system over time. Typical models of dynamic aspects may be behavioral models (describing the behavior of a component or connector over time), interaction models (describing the interactions between a set of components and connectors over time), or data flow models (describing how data flows through an architecture over time).

The static/dynamic distinction is often not a clear line. For example, a system's structure may be relatively stable, but may change occasionally due to component failure, the use of flexible connectors, or architectural dynamism (See Chapter 14). In these cases, models that capture both static and dynamic system aspects may be employed: for example, a (static) base topology may be accompanied by a set of transitions that describe a limited set of changes that may occur to that topology during execution.

There is an important distinction between modeling static and dynamic *aspects* of a system, and using static or dynamic *models*. The former refer to properties of the system being modeled. A static aspect of the system does not change over time, or as the system runs. A dynamic aspect does change. The latter refer to changes to the models themselves. Static models do not change as a result of, e.g., state changes in the running systems that they model. Dynamic models do change. You do not necessarily need dynamic models to capture dynamic aspects of a system. For example, a statechart can capture the behavior of a component over time (a dynamic aspect), but the statechart itself need not change (e.g., acquire new nodes or transitions) as the component executes. Meaningfully analyzing or visualizing characteristics of a system as it runs, however, does generally require the use of dynamic models.

Supporting dynamic models is more difficult than supporting static models. Once developed, static models can be incorporated into a system in "read-only" mode—they are static resources that can be used as a basis for implementation, comparison and analysis. Dynamic models must be

incorporated in "read-write" mode—the system's execution can change the model itself. This requires consistency maintenance mechanisms to keep the model and the system synchronized. For these mechanisms to operate automatically, the model must be stored in a machine-readable and writable form, and the model must be appropriately mapped to the implemented system. Visualizations of the model must also be suitably dynamic, reflecting changes to the model on-the-fly if possible.

### 6.1.5 Functional and Non-Functional Aspects

Architecture can capture both functional and non-functional aspects of a system. Functional aspects relate to *what* a system does. Non-functional aspects relate to *how* a system performs its functions, or to more abstract, harder-to-quantify qualities like usability. A good rule of thumb for thinking about this distinction is that functional aspects of a system can be described using declarative, subject-verb sentences: *the system prints medical records*; non-functional aspects of a system can be described by adding adverbs to these sentences: *the system prints medical records quickly and confidentially*. An extensive survey of non-functional properties from an architectural perspective is contained in Chapter 12.

Because functional aspects are generally more concrete, they are easier to model, and can often be modeled rigorously and formally. Typical functional models of a system might capture what services are provided by different components and connectors, and the interconnections that achieve the overall system functions. They may capture the behavior of components, connectors, or subsystems, describing what functions those elements perform. Functional aspects of a system can be static or dynamic.

Choosing a modeling approach for functional aspects is dependent on the particular aspect of the system being modeled. Any notation must employ a sufficient number of concepts to express and reason about the aspect; the underlying semantics of the approach will determine what kinds of reasoning and analysis can be achieved.

Non-functional aspects of systems are generally less concrete, and this limits the level of detail with which they can be modeled. Models of non-functional aspects of systems may be more informal and less rigorous than functional models, but this does not mean they should not be captured. Often, functional aspects of systems are developed specifically to correspond with or implement non-functional aspects. For example, a non-functional model might simply prescribe that the paycheck processing component should be fast. The functional model of the paycheck component may describe how the paycheck processing component uses caches and local processing—two functional strategies that help to achieve the modeled non-functional aspect.

Much like design rationale, non-functional aspects of systems are difficult to model with rigor. Expressive, free-form notations like natural language are often used for capturing non-functional aspects. It is useful, however, to employ approaches centered on traceability. Traceability models map non-functional properties to functional design decisions that are intended to implement that property; this is a form of design rationale capture as well.

## 6.2 Ambiguity, Accuracy, and Precision

Architectures are abstractions of systems. They capture information about some aspects of the system and leave other aspects out. Ideally, the principal, most important aspects of a system will be well defined by the architecture. The parts that are specified may describe the nominal state of the system and leave out unusual states. This is, to some extent, normal—architectures are not meant to be complete implementations of a system. Consequently, the notations used to capture architectures do not have to be completely unambiguous, accurate and precise.

Three key concepts have to be examined and addressed when developing and assessing the quality of an architectural model: ambiguity, accuracy, and precision.

**Definition.** A model is *ambiguous* if it is open to more than one interpretation.

Incompleteness in models can lead to ambiguity. In general, we attempt to eliminate ambiguity before developing software systems, because conflicting interpretations often lead to bugs and errors. However, the expense of modeling every aspect of a system in its architecture will nearly always outweigh the benefits of doing so. A good guideline is to allow aspects of the system to be ambiguous with the consent of appropriate stakeholders, proceeding when they agree that the architecture is “complete enough” and remaining decisions can be made in a future development activity. While this evaluation proceeds, it is useful to specifically identify and document ambiguous aspects of the architecture as a kind of design rationale.

**Definition.** A model is *accurate* if it is correct, conforms to fact, or deviates from correctness within acceptable limits.

**Definition.** A model is *precise* if it is sharply exact or delimited.

Many conceptions of accuracy and precision, including dictionary definitions, conflate the two terms. Here, we will adopt an interpretation that more clearly delineates them.

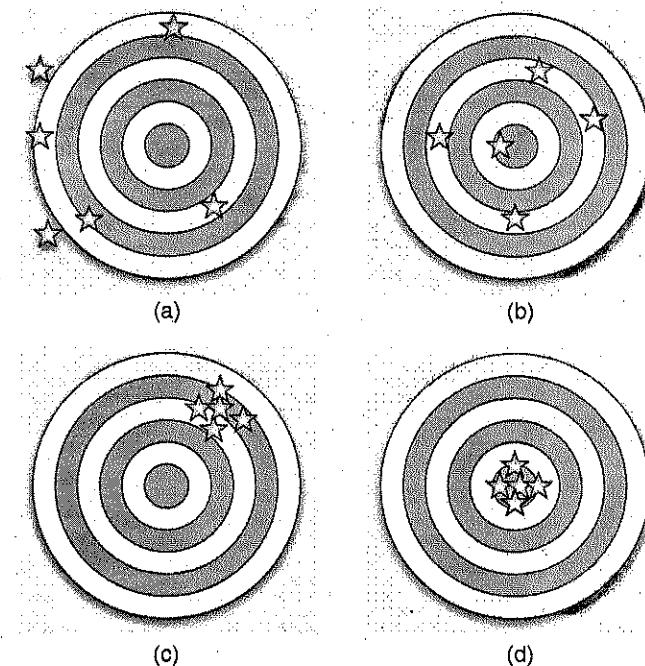


Figure 6-2. A graphical depiction distinguishing accuracy and precision.

Figure 6-2 graphically depicts our distinction between accuracy and precision as a set of targets that have been shot. Consider each shot to be an assertion about a system being designed. Figure 6-2(a) shows a set of shots (assertions) that are neither accurate nor precise: they are not close together nor are they near the target. Architecturally, this represents design decisions that are incoherent or contradictory. Figure 6-2(b) shows shots that are accurate, but not precise: they are clustered around the target, but are not close together. Architecturally, this might be a result of ambiguity or correct descriptions of only some aspects of the system. Figure 6-2(c) shows shots that are precise, but not accurate: they are clustered close together, but they are not near the target. This could be interpreted as design decisions that describe an aspect of the system incorrectly, but in great detail. Figure 6-2(d) shows shots that are both precise and accurate.

In developing an architecture, accuracy should generally be favored over precision. Precision and completeness are, of course, desirable, but are issues that can be resolved during detailed design and implementation.

activities. However, architectures that are inaccurate will generally lead to errors in later development activities.

Notations and modeling approaches can have a significant effect on the ambiguity, accuracy, and precision of models. Some notations include constructs that are purposefully ambiguous—they are intended to be interpreted in the manner most useful to the stakeholders. Other notations are based on formal semantics, and allow unambiguous, precise specifications of certain aspects of a software system. As we have discussed, stakeholders should generally choose notations that allow unambiguous and precise modeling of the aspects of the system *that are the most important*. Since no notation will be comprehensive for modeling every aspect of a system, combinations of notations should be used to capture an architecture.

Ultimately, we use architecture to ensure that the system we are developing attains specific desired qualities.

One of the most common errors in judgment made by decision-makers in software engineering is to assume that creating architecture models in a particular notation will (substantially) guarantee that the developed system achieves certain qualities. This sentiment is embodied in familiar statements like “We know we have a good architecture because we designed it using UML” or “Of course our architecture is reliable—it conforms to DODAF.”

**Sidebar: The Illusion of quality.**

Improving qualities is done by making good design decisions and documenting those decisions with adequate precision. In most notations, it is just as easy to model bad design decisions as good ones. Notations with inherent ambiguities can cause confusion and misunderstandings between stakeholders. This does **not** necessarily mean that these notations are badly designed or unsuitable for use; it simply means that architects and other stakeholders must always keep in mind the scope and limitations of the notations they use. It is not simply a notation, but a notation combined with good visualizations and analysis methods that helps to improve software qualities.

## 6.3 Complex Modeling: Mixed Content and Multiple Views

Architecture models are complex artifacts. They attempt to capture all the design decisions about a system that are important to a wide variety of stakeholders. Additionally, different aspects of the same concept will be captured simultaneously, e.g., a component’s interconnections to other components, as well as its behavior, as well as its version history. There is simply too much information to deal with all at once, and attempting to do

so is not productive: stakeholders generally want to interact with the parts of the architecture that are most important from their own perspective.

In general, no single approach will be able to capture all the aspects of an architecture for a project. This means that various parts of the architecture may have to be modeled using different approaches. These architectures will be captured using *mixed content*, selecting appropriate notations and formalisms for different parts of the architecture. For example, non-functional aspects of a system may be captured using natural language, its structure modeled with a component-connector graph, and various component behaviors using statecharts.

### 6.3.1 Views and Viewpoints

This situation induces the notion of *views* and *viewpoints*.

**Definition:** A *view* is a set of design decisions related by a common concern (or set of concerns).

**Definition:** A *viewpoint* defines the perspective from which a view is taken.

A view is an instance of a viewpoint for a specific system. Put another way, a viewpoint is a filter for information, and a view is what you see when you look at a system through that filter.

For example, consider the domain of systems where software components are distributed across multiple hosts. The *deployment viewpoint* is a perspective on such systems that captures design decisions related to how components are assigned to hosts. The *deployment view* of a particular system captures how components are assigned to hosts for that particular system.

Figure 6-3. The deployment views of the architectures of two different systems.

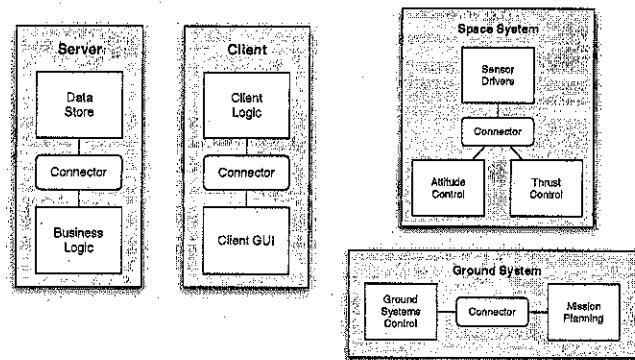


Figure 6-3 shows the deployment view of two different systems. Figure 6-3(a) shows the deployment view of a client-server system. Figure 6-3(b) shows the deployment view of a distributed space-ground system like the Lunar Lander. However, both of these views are taken from the *deployment viewpoint*: that is, they both capture design decisions dealing with the deployment of components onto hosts.

In general, viewpoints capture subsets of an architecture related to one concern. Examples of viewpoints that are commonly captured include:

- **Logical Viewpoints:** Capture the logical (often software) entities in a system and how they are interconnected.
- **Physical Viewpoints:** Capture the physical (often hardware) entities in a system and how they are interconnected.
- **Deployment Viewpoints:** Capture how logical entities are mapped onto physical entities.
- **Concurrency Viewpoints:** Capture how concurrency and threading will be managed in a system.
- **Behavioral Viewpoints:** Capture the expected behavior of (parts of) a system.

It is also possible for multiple views to be taken from the same viewpoint for the same system. That is, there might be multiple deployment views for a single system, with different levels of detail. One view might show only top-level components, while another might show both top-level components as well as subcomponents and additional internal structure.

The use of views and viewpoints in modeling is important for several reasons:

- They provide a way to limit presented information to a cognitively-manageable subset of the architecture.
- They display related concepts simultaneously.
- They can be tailored to the needs of specific stakeholders.
- They can be used to display the same data at various levels of abstraction.

### 6.3.2 Consistency among Views

Architectural models capture multiple views simultaneously. Often, the same (or related) information will be present in two or more views. This immediately gives rise to an important question: are these views consistent with one another? To answer this, we must consider what consistency means with respect to architectural views.

Views are *consistent* if the design decisions that they contain are compatible. Alternatively, consistency can be seen as the absence of inconsistency. An *inconsistency* occurs when two views assert design decisions that cannot both be simultaneously true.

Many kinds of inconsistency can arise. Some kinds of inconsistency that might occur in a multiple-view architecture description include:

**Direct inconsistencies:** Two views assert directly contradictory propositions, e.g. “the system runs on two hosts” and “the system runs on three hosts.” These inconsistencies can often be detected by automatic mechanisms that employ appropriate constraints and rules.

**Refinement inconsistencies:** Two views of the same system at different levels of detail assert contradictory propositions. For example, a “top level” structural view contains a component that is absent from a structural view that includes subarchitectures. These inconsistencies can also be automatically detected with appropriate consistency rules.

**Static aspects vs. dynamic aspects:** A view of a static aspect of a system conflicts with a view of a dynamic aspect. For example, a message sequence chart view might depict the handling of messages by a component that is not contained in the structural view. These inconsistencies can be somewhat harder to automatically detect, depending on how explicit the dynamic aspect’s specification is.

**Dynamic aspects:** Two views of dynamic aspects of the system conflict. For example, a message sequence chart depicts a specific interaction between components that is not allowed by the behavioral specifications contained in those components’ statecharts. These inconsistencies are

often extremely difficult to detect automatically because it would require extensive state exploration or simulations.

**Functional vs. non-functional aspects:** A non-functional property of a system prescribed by a non-functional view is not met by the design expressed in functional views of a system. For example, a non-functional view may express that a system should be robust enough to recover from a server failure, but the physical view of the system may show only a single server with no evidence of failure-handling machinery. These inconsistencies are the most difficult to detect because the problem is equivalent to designing a system that embodies specified qualities.

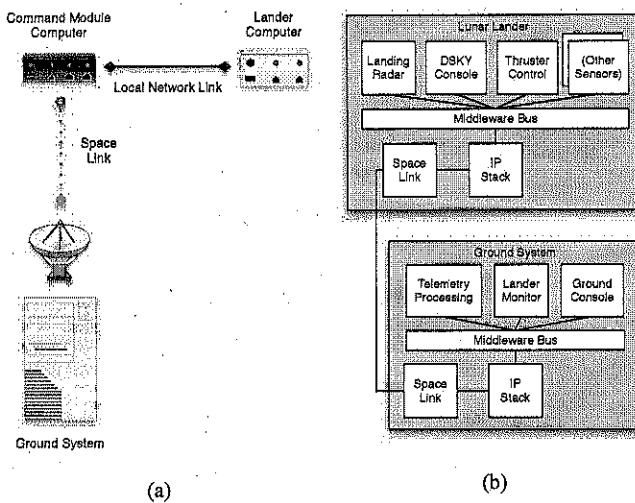


Figure 6-4: A Lunar Lander system's physical view (a) and logical view (b).

Figure 6-4 shows two hypothetical views of a distributed Lunar Lander system. The physical view (a) depicts three hosts, a Ground Station, a Command Module Computer, and a Lander Computer. However, the deployment view (b) shows components assigned to only two hosts, a Ground Station and a Lunar Lander. It is fairly easy to see that something is not right here—there is an inconsistency between the physical and deployment view. The inconsistency fits our above definition—the physical view asserts the design decision that Lunar Lander runs on two hosts, while the deployment view asserts the decision that Lunar Lander runs on three.

This inconsistency is relatively easy to spot just by looking. However, other, subtler inconsistencies (such as inconsistencies between different behavioral specifications of an architecture) are harder to detect and more costly to fix.

Identifying, detecting, and resolving inconsistencies among views is a difficult problem. First, stakeholders must agree on what ‘consistency’ means for their particular choice of views and modeling notations. Then, strategies must be employed to locate and deal with inconsistencies. These can range from manual approaches such as inspections and checklists to automated approaches such as model checking and simulation. Chapter 8, which covers architectural analysis, will discuss specific approaches for dealing with inconsistency in detail.

Inconsistency is generally, but not always, undesirable. Inconsistencies will arise as a natural part of doing exploratory design—as you design an architecture, parts of it may be temporarily inconsistent as the design evolves. Sometimes, inconsistencies are left in an architecture deliberately upon agreement of the stakeholders to deal with a special case, or because repairing the inconsistency would be too costly.

## 6.4 Evaluating Modeling Techniques

In the past sections, we have explored a number of dimensions that can be used to characterize different modeling techniques. These dimensions can be straightforwardly turned into a rubric for critically thinking about and evaluating different modeling techniques.

<b>Scope and Purpose</b>	What is the scope of the technique? What is it intended to model and what is it <i>not</i> intended to model?
<b>Basic Elements</b>	What are the basic elements or concepts (e.g., the ‘atoms’) in the technique? How are these modeled?
<b>Style</b>	To what extent does the technique support modeling of stylistic constraints, and for what kinds of styles?
<b>Static and Dynamic Aspects</b>	To what extent does the technique support modeling static aspects of architecture? To what extent does it support modeling dynamic aspects of architecture?
<b>Dynamic Modeling</b>	To what extent can the model be changed to reflect changes as a system executes?
<b>Non-Functional Aspects</b>	To what extent does the technique support modeling non-functional aspects of architecture? (Here, we leave out functional aspects because we assume that those will be adequately covered by other parts of the rubric).
<b>Ambiguity</b>	What measures does the approach take to limit (or allow)

	ambiguity?
Accuracy	To what extent does the approach provide support for determining the correctness of models?
Precision	At what level of detail can the various aspects of architecture be modeled?
Viewpoints	What viewpoints does the model support?
View Consistency	To what extent does the approach provide support for determining the consistency of different views expressed in a model?

This rubric will be applied to several techniques in the remainder of this chapter.

## 6.5 Specific Modeling Techniques

Architects have at their disposal a panoply of available notations and techniques for modeling different aspects of architectures. These techniques vary along many dimensions: what they can model, how precisely they can capture architectural semantics, how good their tool support is, and so on. In general, a combination of these methods will be most effective in capturing all relevant architectural aspects. What methods are used, and for what purposes, will be largely up to a system's architects and stakeholders. While many approaches for modeling architectures are broadly-scoped and applicable to many systems in many domains, it is important not to become dogmatically attached to any one approach.

The next sections will discuss and evaluate various approaches that can be used for modeling software architectures. For each modeling approach, a simple three-component version of the Lunar Lander application will be presented using that approach.

### 6.5.1 Generic Techniques

These techniques are often used to describe (parts of) a software architecture, although they were not specifically developed or adapted for this purpose. As such, they tend to be flexible but have few semantics.

#### Natural Language

Natural languages, such as English, are an obvious way to document architectural design decisions. Natural language modeling is expressive, but is ambiguous, non-rigorous, and non-formal. Natural language cannot be processed and understood by machines, and thus can only be checked and inspected by humans.

Despite these drawbacks, natural-language modeling can be the best way to capture some aspects of an architecture. For example, some non-functional requirements are best captured using natural language, since these are often subjective. Natural language is accessible to all stakeholders, and can be manipulated with common tools like word processors.

An alternative to using pure natural language is to use a restricted form of it. Users can create and consistently employ a dictionary of terms in order to limit certain kinds of difficulties (e.g., using different terms for the same concept, or lack of clarity). "Statement templates," which are statements or paragraphs in natural language with 'fill-in-the-blanks' parameters can be another way to increase rigor in natural language. However, overusing this strategy has a negative effect—essentially, it creates a domain-specific language without any of the flexibility benefits of natural language.<sup>8</sup>

#### Evaluation Rubric for Natural Language

Scope and Purpose	Describing arbitrary concepts with an extensive vocabulary, but in an informal way.
Basic Elements	Any concepts required, no special support for any particular concept.
Style	Stylistic concepts can be described by simply using more general language.
Static and Dynamic Aspects	Both static and dynamic aspects of systems can be modeled.
Dynamic Modeling	Models must be changed by humans and can be rewritten with a tool such as a word processor, but there is no feasible way to tie these models to implementation.
Non-Functional Aspects	Expressive vocabulary available for describing non-functional aspects of systems (although there is no support for verifying them).
Ambiguity	Plain natural language is perhaps the most ambiguous notation available for expressing architectures; techniques

<sup>8</sup> In the early days of computing, some programming language designers believed that programming languages could be improved by making them more like natural language with added syntactic rigor. Thus, languages like COBOL included statements like "MULTIPLY X BY 5 GIVING Z" instead of the terser "z = x \* 5." Such techniques have fallen out of favor, as they only served to make programs more verbose.

	like statement templates and well-defined dictionaries of terms can be used to reduce ambiguity.
<b>Accuracy</b>	Correctness must be evaluated through manual reviews and inspections, and cannot be automated.
<b>Precision</b>	Additional text can be used to describe any aspect of architecture in greater detail.
<b>Viewpoints</b>	All viewpoints (but no specific support for any viewpoint).
<b>View Consistency</b>	Correctness must be evaluated through manual reviews and inspections, and cannot be automated.

**Lunar Lander in natural language:** Here, we introduce a simple three-component version of the Lunar Lander application that will be used throughout the remainder of this chapter to illustrate the use of different modeling approaches. The Lunar Lander application might be described in natural language as follows:

*"The Lunar Lander application consists of three components: a data store component, a calculation component, and a user interface component.*

*The job of the data store component is to store and allow other components access to the height, velocity, and fuel of the lander, as well as the current simulator time.*

*The job of the calculation component is to, upon receipt of a burn-rate quantity, retrieve current values of height, velocity, and fuel from the data store component, update them with respect to the input burn-rate, and store the new values back. It also retrieves, increments, and stores back the simulator time. It is also responsible for notifying the calling component of whether the simulator has terminated, and with what state (landed safely, crashed, and so on).*

*The job of the user interface component is to display the current status of the lander using information from both the calculation and the data store components. While the simulator is running, it retrieves the new burn-rate value from the user, and invokes the calculation component."*

The above description tells the reader a fairly significant amount about the Lunar Lander system. For example, the structure of the components and their dependencies is explicitly stated, as well as a description of their behaviors, inputs, outputs, and general responsibilities. The description stops short of specifying certain details that are required for implementing the system. For example, it does not explain the algorithm the *calculation* component uses for its computations, the particular formats of the

**Figure 6-5.** Lunar Lander specification in natural language (American English).

different data values, anything about the connectors between the components, or what the user interface should look like.

Many different implementations could satisfy this architectural specification, and they may not all function identically. This is partially due to the nature of architectural models in general—they document *principal* design decisions, not all design decisions. It is also partially due to the ambiguity inherent in natural language specifications. This specification is also probably not the tersest or most understandable way of expressing aspects of this system like its structure—readers of the above specification are likely to build up a mental dependency graph of the lander’s constituent component as they read, since one is not provided.

**Takeaways:** Natural language should be used as an adjunct to more rigorous and formal languages, for aspects of architecture where formalism is infeasible or unnecessary. It is particularly good for specifying non-functional properties in a way that almost no other language can match.

#### Informal Graphical "PowerPoint"-style Modeling

Tools such as Microsoft PowerPoint [192] and OmniGraffle [281] provide users the ability to create decorative diagrams of interconnected shapes. These tools have the advantage that they are ubiquitous and it is easy to use them to create aesthetically pleasing diagrams. The size limitations of such diagrams (one slide, one sheet of paper) help to ensure that they remain at a suitably abstract level.

The main drawback to using these tools is that they create diagrams that capture few (if any) semantics. This makes it difficult to reliably interpret the meaning of the diagrams, undermining the key advantages of using an architecture in the first place (communication, analysis, and so on). While these tools are good for early prototyping and exploration, users must be cautious because it is often difficult or impossible to transfer the diagrams into a more semantically precise format. These diagrams can be improved with the addition of artifacts describing the specific semantics of diagrammatic elements.

#### Evaluation Rubric for "PowerPoint"-style Modeling

<b>Scope and Purpose</b>	Arbitrary diagrams composed of graphical and textual elements, with few restrictions on them.
<b>Basic Elements</b>	Geometric shapes, splines, text strings, clip art.
<b>Style</b>	In general, no support.
<b>Static and Dynamic</b>	Because these models lack architectural semantics, there is

<b>Dynamic Aspects</b>	no notion of modeling static or dynamic aspects of systems.
<b>Dynamic Modeling</b>	Model formats are generally proprietary and difficult to change outside of their native environment. However, some environments expose externally callable interfaces that allow models to be manipulated programmatically (e.g., PowerPoint exposes its models through a COM interface).
<b>Non-Functional Aspects</b>	Non-functional aspects can be modeled using natural-language decorations on diagrams.
<b>Ambiguity</b>	As with natural language, ambiguity can be controlled through the use of a controlled symbolic vocabulary or dictionary.
<b>Accuracy</b>	In general, correctness is determined through manual inspection and cannot be automated.
<b>Precision</b>	Modelers can choose an appropriate level of detail; however, they are generally limited by the amount of information that can fit on one diagram or slide.
<b>Viewpoints</b>	Because these models lack architectural semantics, there is no direct support for multiple viewpoints. In theory, a model can show any viewpoint.
<b>View Consistency</b>	In general, consistency is determined through manual inspection and cannot be automated.

**Lunar Lander in PowerPoint:** There are many ways to express the Lunar Lander architecture in a tool like Microsoft PowerPoint, limited only by the symbol palette available in the tool. A Lunar Lander architecture in PowerPoint might look like this:

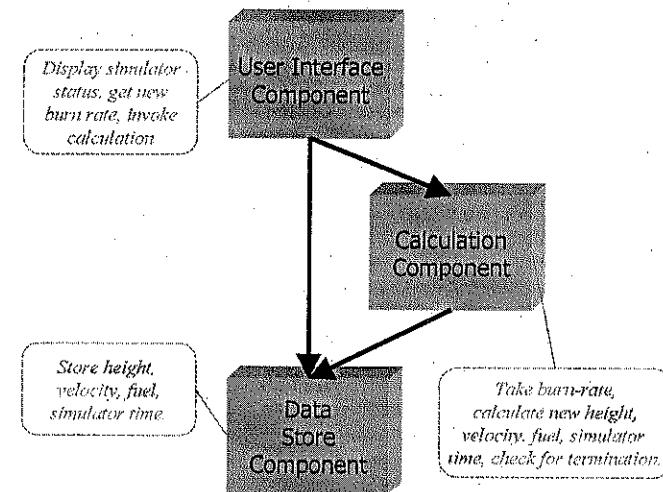


Figure 6-6. Lunar Lander architecture in PowerPoint

As with most PowerPoint architecture diagrams, the particular symbology used is not directly explained—there is no underlying semantic model (other than the reader's expectations) through which to interpret this diagram. The meanings of the three-dimensional boxes, the arrows, and the rounded rectangles are not provided. More serious modeling efforts might provide a symbolic dictionary to accompany such a diagram.

The intended interpretation is that the three-dimensional boxes are software components, the arrows indicate invocation dependencies, and the rounded rectangles are commentary on the intended behavior and responsibilities of the components. Assuming that the reader correctly interprets the meanings of the symbols, this model is easier to understand in certain ways than the natural language model above. For example, the componentization of the system and the component dependencies are immediately obvious, and the behaviors are visually connected to the components.

**Takeaways:** PowerPoint and similar tools are seductive because they make it very easy to create graphical diagrams. However, great care should be taken in using PowerPoint diagrams as part of any official architecture description—they can be valuable for early ‘back-of-the-napkin’ architecture descriptions, but as soon as basic decisions are made, more rigorous notations should be employed for real architecture capture.

### The Unified Modeling Language (and its Cousins)

UML, the Unified Modeling Language [24], is the most popular notation for writing down software designs. It is ‘unified’ in that it combines concepts from earlier notations such as Booch diagrams [22], Rumbaugh’s OMT [247], Jacobson’s OOSE [142], and Harel’s Statecharts [111]. UML’s main strengths are its large variety of modeling constructs and viewpoints, extensive tool support, and widespread adoption.

UML is a massive notation about which entire books can be (and have been) written. We summarize its role as an architectural modeling language here. Further information about UML as a standard for software and system development is presented in Chapter 16.

UML is an inherently graphical notation, with views consisting of textually annotated graphical symbols. It provides its users with an extremely wide variety of modeling constructs and concepts. UML 2.0 includes 13 different viewpoints, called ‘diagrams’ in UML parlance. These viewpoints cover many of the dimensions identified earlier in this chapter—basic architectural elements, stylistic constraints, static and dynamic aspects of systems, and so on.

Much debate has ensued over the years as to UML’s suitability for modeling software systems at the architecture level. Early versions of UML (1.0 and 1.1) [23] had a strong focus on detailed design—below the level of architectural constructs such as components and connectors. It was biased toward the design of object-oriented systems that communicate primarily through procedure calls. UML 2.0 significantly expanded UML to provide much better support for architecture-level constructs. Existing viewpoints were extended with new elements, and entirely new viewpoints were added.

UML’s broad range of diagrams makes it an attractive option for modeling all kinds of software systems. However, it is vitally important for architects not to get ‘locked in’ to UML as their one and only modeling solution for architectures, or to overestimate the benefits conferred by using UML.

UML’s viewpoints remain mostly focused on design. In many ways, these viewpoints still retain an inherent bias to modeling object-oriented systems. Some of the viewpoints extend into other lifecycle activities, with limited support for capturing requirements and implementation-related aspects. Explicit support is minimal for activities such as testing and maintenance and meta-activities like management. Architectural decisions can affect any of these aspects of development, so it is often useful to incorporate additional notations to capture a complete architecture.

Understanding the semantics of UML diagrams is key to making them useful in describing architectural design decisions. UML is more precise than arbitrary diagrams that would be produced in PowerPoint or Visio. However, it has been designed to be purposefully ambiguous in many respects so as to increase its generality.

Figure 6-7. A UML class diagram showing a dependency between two components.



For example, the dashed open-headed arrow is a ‘dependency’ arrow. It indicates that the element at the tail end of the arrow has some dependency on the element at the head end of the arrow. Figure 6-7 shows a simple UML component diagram with two components. The dashed arrow indicates that the *Calculation* component is dependent on the *Data Store* component. However, this could mean any number of things, e.g.:

- Some element of *Calculation* calls *Data Store*.
- Instances of *Calculation* contain a pointer or reference to an instance of *Data Store*.
- *Calculation* requires *Data Store* to compile.
- *Calculation*’s implementation has a method that takes an instance of *Data Store*’s implementation as a parameter.
- *Calculation* can send messages to *Data Store*.

And so on, and so on. Most constructs in UML are similarly semantically ambiguous (it is even unclear what the classes in the above diagram refer to: they could be classes in an object-oriented programming language, C modules, Web services, etc.)

This approach gives UML great flexibility but limits its semantic precision. Fortunately, UML includes facilities that allow its users to define new attributes (called *stereotypes* and *tagged values*) and constraints that can be applied to existing elements to specialize them. A collection of these additional attributes and constraints is known as a UML profile. Profiles are generally designed for specific applications, product lines, or domains, and serve to increase the semantic precision of UML diagrams within that scope.

Figure 6-8. UML class diagrams with more specific semantics provided by using stereotypes.

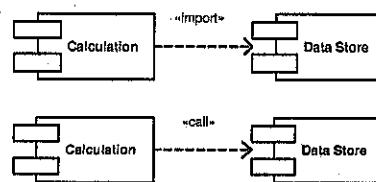


Figure 6-8 shows two variants of the component diagram in Figure 6-7. Each of these uses a UML *stereotype* to provide additional detail about the meaning of the dependency arrow. This does not make the dependency arrow completely unambiguous, however—understanding it still relies on the reader's interpretation of 'import' or 'call.' The top diagram indicates that *Calculation* imports *Data Store*. The bottom diagram indicates that *Calculation* calls *Data Store*. The available selection of stereotypes (and their specific meanings) are defined by the UML profile in use.

UML diagrams alone do not carry enough information to completely interpret them. Stakeholders may make agreements among themselves about how to interpret particular aspects of UML diagrams on a project, and document these agreements in external natural-language documents. Stakeholders should also strongly consider defining or selecting a profile with documented interpretations for the included stereotypes, tagged values, and constraints.

#### Evaluation Rubric for UML

<b>Scope and Purpose</b>	Capture design decisions for a software system using up to 13 different diagram types.
<b>Basic Elements</b>	A multitude—classes, associations, states, activities, composite nodes, constraints (in OCL) and so on.
<b>Style</b>	Stylistic constraints can be expressed in the form of OCL constraints or by providing (partial) models in one of the many viewpoints.
<b>Static and Dynamic Aspects</b>	Includes a number of diagrams for modeling both static (e.g., class diagram, object diagram, package diagram) and dynamic aspects (e.g., state diagram, activity diagram) of systems.
<b>Dynamic Modeling</b>	Depends on the modeling environment; in practice very few systems are tied directly to a UML model such that the UML model can be updated as they run.
<b>Non-Functional</b>	No direct support, except perhaps in textual annotations.

Aspects	
<b>Ambiguity</b>	In general, UML elements can mean different things in different contexts. Ambiguity can be reduced through the principled use of UML profiles, including stereotypes, tagged values, and constraints.
<b>Accuracy</b>	Aside from OCL constraint checking and basic well-formedness checks (e.g., no broken links, every element has a name, etc.), there is no standard for assessing the accuracy of a UML model.
<b>Precision</b>	Modelers can choose an appropriate level of detail; UML offers wide flexibility in this regard.
<b>Viewpoints</b>	Each kind of diagram represents at least one possible viewpoint; through overloading or partitioning, one diagram can be used to capture multiple viewpoints as well.
<b>View Consistency</b>	Very little support is provided for checking consistency among diagrams; OCL constraints can be used in a very limited fashion for this purpose.

**Lunar Lander in UML:** UML provides many possible viewpoints from which to model the Lunar Lander architecture. Which of these are used, and to what depth, depends on the stakeholders involved and their concerns. Here, we will use a component, statechart, and sequence diagram that will describe the Lunar Lander at roughly the same level of detail as has been shown above in the natural language and PowerPoint-style examples. The component diagram for Lunar Lander might look like this:

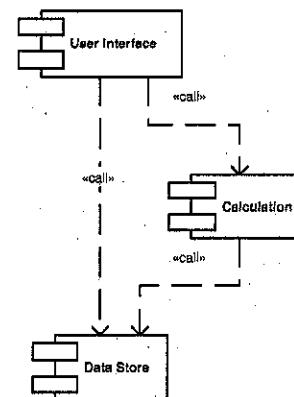


Figure 6-9. Lunar Lander component diagram in UML.

This diagram looks very similar to the PowerPoint-style diagram, because it largely depicts the same aspect of the architecture. Unlike the PowerPoint diagram, though, this diagram has a rigorous syntax and an underlying semantic basis. The symbols used for components and dependencies are standard and documented as part of the UML specification. This is not to say that the diagram is completely unambiguous—for example, the diagram says nothing about what a component is in this context, or when and how the calls among components are made. Some of these details can be specified in other UML diagrams. The behavior of the system might be specified in a UML statechart diagram, as follows:

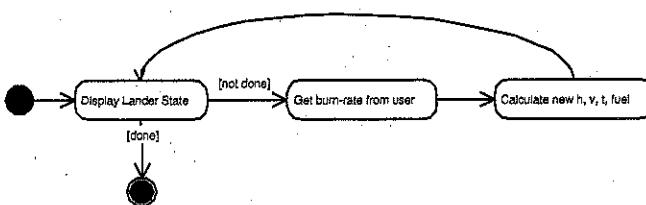


Figure 6-10. Lunar Lander statechart diagram in UML.

This diagram describes the behavior of the system. The start state is indicated by the plain dark circle, and the end state is indicated by the outlined dark circle. Each rounded rectangle represents a state of the system, and arrows represent transitions between the states. The conditions in square brackets indicate guards that constrain when state transitions may occur.

This statechart indicates that the Lander system begins by displaying the lander state. If the simulation is done, the simulator will stop. Otherwise, the system will request a burn-rate from the user. It will then calculate the new simulator state and display it. This control loop will repeat until the simulation is done.

While this statechart diagram provides a more rigorous and formal description of the system behavior than either the natural language or PowerPoint-style architecture description, it leaves out some important details contained in both those descriptions—namely, which components perform the specified actions. This information can be described in another UML diagram, such as a UML sequence diagram. A sequence diagram for the Lunar Lander application might look like this:

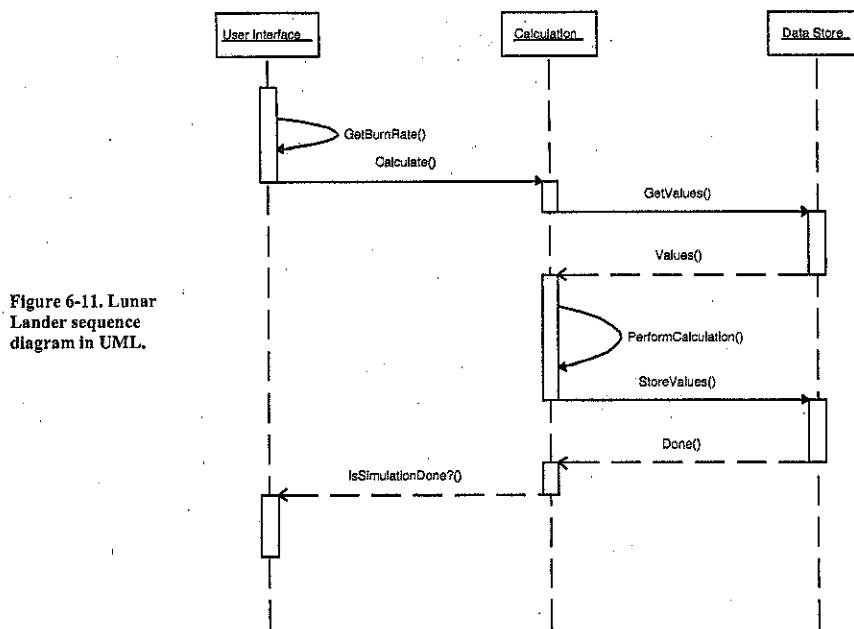


Figure 6-11. Lunar Lander sequence diagram in UML.

This diagram depicts a particular sequence of operations that can be performed by the three Lunar Lander components. Sequence diagrams such as this one are not intended to capture all the behavior of a system; rather, they are used to document particular scenarios or use cases. The above diagram depicts one nominal scenario—*User Interface* gets a burn rate from the user, *Calculation* retrieves the state of the lander from the *Data Store* and updates it, and then returns the termination state of the lander to *User Interface*.

Figure 6-9, Figure 6-10, and Figure 6-11 represent three different views of the Lunar Lander architecture. These views capture both static (structural) and dynamic (behavioral) aspects of the system. A natural question to ask is whether these views are consistent with one another. There is no standard way to answer this question, as there is no concrete notion of consistency in UML. Instead, we have to establish our own criteria for consistency and check the views against these criteria. For example, we could check whether each component in the component diagram is represented in the sequence diagram, and whether the calls in the sequence diagram are allowed by the dependency arrows in the component diagram.

Checking the consistency of the above statechart and sequence diagrams is a more difficult task. These two diagrams model behavioral aspects of the architecture at substantially different levels—the statechart describes the overall functioning of the system, while the sequence diagram shows a particular scenario and includes lower-level data like the individual operations that make up the depicted interaction. In this case, inspections and stakeholder agreement are probably the best way to determine the consistency of the diagrams.

**Takeaways:** UML is a syntactically rich notation with extensive tool support for editing. As a way of expressing architectural design decisions, it is superior to a symbols-only notation like PowerPoint's. However, UML's purposeful ambiguity about the meaning of most of its symbols leaves it open for abuse. Even well-intentioned development groups can fall victim to inconsistent interpretations of the same diagrams. This is particularly dangerous when stakeholders are from diverse backgrounds or geographic locations. When UML is employed, profiles must be developed and used to ensure consistent modeling, although this does not necessarily guarantee unambiguous interpretations. Profiles are not a panacea.

### 6.5.2 Early Architecture Description Languages

The 1990s spawned nearly a decade of research on how to best capture software architectures. The result of this research was a proliferation of architecture description languages (ADLs), notations developed specifically for software architecture modeling.

There is no established ‘litmus test’ to determine whether a particular notation is an ADL or not, and there is significant variability in the spectrum of languages that are identified by their creators as ADLs. Medvidovic and Taylor [189] surveyed a wide variety of ADLs and found that the common denominator was explicit support for modeling:

- Components
- Connectors
- Interfaces
- Configurations (or links)

Additionally, these languages tend to be semantically precise, but lack breadth and flexibility. There has been significant debate about whether design notations like UML are ADLs. Certainly, UML (especially UML 2.0) has the ability to model these basic constructs, but its initial purpose was not necessarily to model architecture. It is fair to say that UML can be used as an ADL.

The early “first generation” architecture description languages described in this chapter are, for the most part, research projects. None of these is still used actively in practice. We present them here because of their unique contributions to the field of architecture modeling, but their use in practice may prove difficult for extrinsic reasons (e.g., lack of current tool support).

Some ADLs in this category include:

#### Darwin

Darwin [175] is a general-purpose architecture description language for specifying the structure of systems composed from components that communicate through explicit interfaces. Darwin has a canonical textual representation in which components and their interconnections are described. There is an associated graphical visualization that depicts Darwin configurations in a more accessible but less precise way.

In Darwin, systems are modeled as a set of interconnected components. There is no notion of explicit software connectors in Darwin, but a component that facilitates interactions could be interpreted as a connector. Darwin components expose a set of *provided* and *required* services, sometimes called *ports*. Services in Darwin correspond to our notion of provided and required architectural interfaces. Configurations are specified by a set of bindings between interfaces. Darwin also has support for hierarchical composition—that is, components that have internal structures also consisting of components, services, and bindings.

#### Evaluation Rubric for Darwin

<b>Scope and Purpose</b>	Structures of distributed systems that communicate through well-defined interfaces.
<b>Basic Elements</b>	Components, interfaces (required and provided), links (called bindings), hierarchical composition.
<b>Style</b>	Limited support through the use of parameterizable constructs.
<b>Static and Dynamic Aspects</b>	Support for static structural views, additional support for dynamic architectures (e.g., those that change at run-time) through lazy and direct dynamic instantiation and binding.
<b>Dynamic Modeling</b>	Not available.
<b>Non-Functional Aspects</b>	Not available.
<b>Ambiguity</b>	How Darwin's constructs (e.g., components, interfaces) can

	be composed and used within a Darwin model is well-defined. Their external meaning (e.g., what it means to be a component or a interface) is subject to stakeholder interpretation.
Accuracy	Darwin can be modeled in the formalism known as the <i>pi</i> -calculus, which allows the models to be checked for internal consistency.
Precision	Detail limited to structural elements and their interconnections.
Viewpoints	Structural viewpoints, deployment viewpoints through the use of hierarchical composition.
View Consistency	Not available.

**Lunar Lander in Darwin:** Darwin is primarily a structural description notation, and we can use it to describe the three-component Lunar Lander's structure. The textual visualization of Lunar Lander in Darwin might be expressed as follows:

```

component DataStore{
    provide landerValues;
}

component Calculation{
    require landerValues;
    provide calculationService;
}

component UserInterface{
    require calculationService;
    require landerValues;
}

component LunarLander{
inst
    U: UserInterface;
    C: Calculation;
    D: DataStore;
bind
    C.landerValues -- D.landerValues;
    U.landerValues -- D.landerValues;
    U.calculationService -- C.calculationService;
}

```

Figure 6-12. Lunar Lander architecture in Darwin's textual visualization.

Here, each component is described with explicit provided and required interfaces. The overall application structure is defined using a top-level component with an internal structure—that is, the Lunar Lander application itself is a component containing the *User Interface*,

*Calculation*, and *DataStore* components. As stated above, Darwin also has a canonical graphical visualization; the above model expressed in that visualization might look like this:

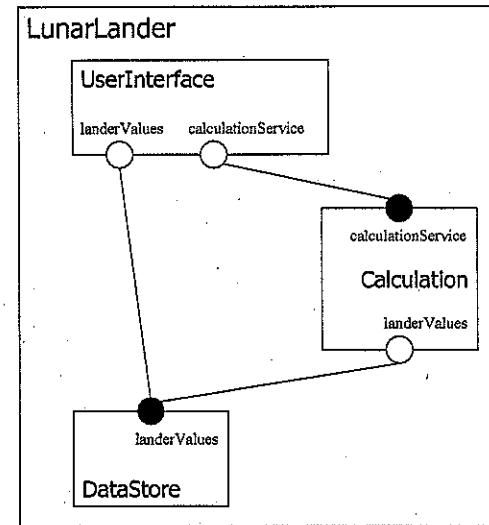


Figure 6-13. Lu  
Lander archite  
Darwin's graph  
representation.

The use of multiple visualizations to depict the same architectural model will be discussed extensively in the next chapter.

One of the most interesting aspects of Darwin is the set of constructs with which configurations of components can be specified. Many declarative ADLs simply enumerate all the components and bindings in an architecture one-by-one (and Darwin supports this—the above model of Lunar Lander uses Darwin in this way). However, Darwin also supports the creation of configurations using programming language-like constructs such as loops. For example, consider a Web application where a number of identical clients are all connecting to the same Web server. We might model this architecture in Darwin as follows:

```

component WebServer{
    provide httpService;
}

component WebClient{
    require httpService;
}

```

Figure 6-14. Model of a  
mult-client Web  
application in Darwin's  
textual visualization.

```

}
component WebApplication(int numClients){
    inst S: WebServer;
    array C[numClients]: WebClient;
    forall k:0..numClients-1{
        inst C[k] @ k;
        bind C[k].httpService -- S.httpService;
    }
}

```

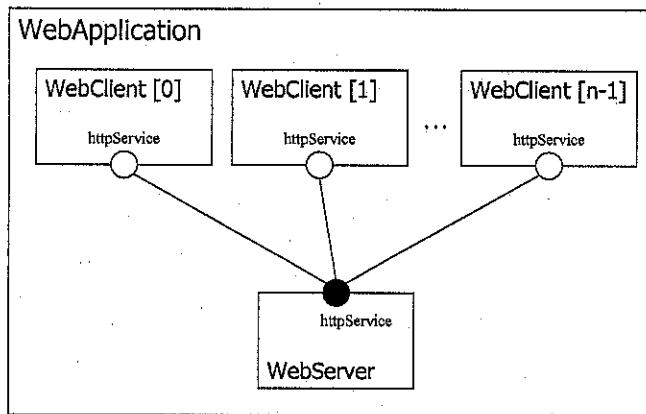


Figure 6-15. Model of a multi-client Web application in Darwin graphical visualization.

In this Darwin model, the actual number of clients is parameterizable. Using these facilities, relatively terse models can be constructed that describe a wide variety of architectures without a great deal of redundancy in the model.

**Takeaways:** Darwin represents a more rigorous and formal way of capturing an architecture's structure than any notation we have seen thus far in the chapter. It provides a well-defined textual syntax with an associated graphical visualization, along with specific, well-defined semantics. It is not overly complex and can be understood by straightforward reading. For structural modeling, Darwin is an excellent choice. For modeling other aspects of architecture, however, other notations should be used.

### Rapide

Rapide [170] is an architecture description language developed to specify and explore dynamic properties of systems composed of components that communicate using events. In Rapide, events are simply the result of an activity occurring in the architecture. Traditional procedure calls are expressed as a pair of events: one for the call and one for the return value.

The power of Rapide comes from its organization of events into Partially Ordered SETs, called POSETs [168]. Rapide components work concurrently, emitting and responding to events. There are causal relationships between some events: for example, if a component receives event A and responds by emitting event B, then there is a causal relationship from A → B. Causal relationships between events A and B in Rapide are defined by (from the Rapide documentation):

- A and B are generated by the same process, or
- A process is triggered by A and then generates B, or
- A process generates A and then assigns to a variable v, another process reads v and then generates B, or
- A triggers a connection which generates B or
- A precedes C which precedes B (transitive closure).

As a program runs, its various components will generate a stream of events over time. Some of these events will be causally related (by one of the above relationships). Some of them may occur around the same time as other causally related events, but be unrelated.

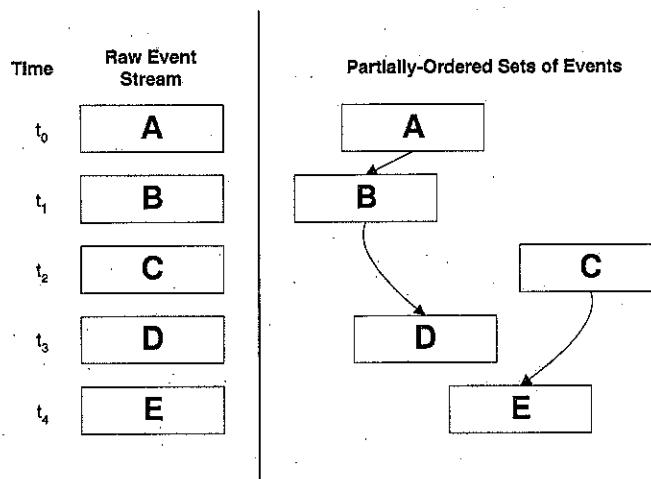


Figure 6-16. Partially ordered sets of events.

Figure 6-16 depicts this situation. The left portion of the figure shows the raw event stream over time: components in the architecture send events *A*, *B*, *C*, *D*, and *E* at times  $t_0$  through  $t_4$ , respectively. These events are temporally ordered, but not causally ordered. The right portion of the figure shows the causal ordering of the events. Here, there are two partial order sequences: one consisting of events *A*, *B*, and *D*, and one consisting of events *C* and *E*. This is called a *partial order* because not all the events are causally ordered with respect to one another. The fact that *B* occurred earlier in time than *C* is only a coincidence—an accident of the scheduler: *C* could have just as easily occurred before *B*.

Because of the focus on events that occur at run-time, Rapide focuses on capturing dynamic aspects of software architectures. Architecture specifications in Rapide are interesting because they are *executable*. Rapide is accompanied by a tool that allows users to execute the architecture description, in effect simulating the operation of the described system. The result is a graph of events similar to the one depicted above in Figure 6-16, showing events as nodes and causal orderings as directed edges.

#### Evaluation Rubric for Rapide

Scope and Purpose	Interactions between components in terms of partially-ordered sets of events.
-------------------	---

Basic Elements	Architectures (structures), interfaces (components), actions (messages/events), and operations describing how the actions are related to one another.
Style	Not available.
Static and Dynamic Aspects	Interconnections among components capture static structure of the architecture, actions and behaviors capture dynamic aspects of the architecture.
Dynamic Modeling	Architectural models do not change during run-time, although some tools provided limited animation capabilities.
Non-Functional Aspects	Not available.
Ambiguity	The semantics of the behaviors are well-defined.
Accuracy	An automatic simulator produces results that can be examined to determine if the architecture's behavior matches expectations. Rapide constraints can also be checked automatically for violations.
Precision	Interconnections and behaviors in terms of event exchanges can be modeled in detail.
Viewpoints	A single structural/behavioral viewpoint.
View Consistency	There is no way to automatically check view consistency (e.g., multiple models describing the same architecture). Inspections can be used to check for consistency across simulator outputs.

**Lunar Lander in Rapide:** The description of Lunar Lander in Rapide looks, on the surface, similar to a Darwin description: a textual notation resembling a programming language is used to define the components and their interface operations. However, the Rapide description also includes behavioral information. This information is used, along with the application structure, to generate event graphs. Since Rapide is optimized for operating on concurrent applications where multiple threads of control interact, we will use it to evaluate a cooperative two-player version of Lunar Lander.

```
type DataStore is interface
    action in SetValues();
    out NotifyNewValues();
    behavior
    begin
        SetValues => NotifyNewValues();
    end DataStore;
```

Figure 6-17.  
Cooperative two-player  
Lunar Lander  
Architecture in Rapide

```

type Calculation is interface
    action in SetBurnRate();
    out DoSetValues();
    behavior
        action CalcNewState();
    begin
        SetBurnRate => CalcNewState(); DoSetValues();;
    end Calculation;

type Player is interface
    action out DoSetBurnRate();
    in NotifyNewValues();
    behavior
        TurnsRemaining : var integer := 1;
        action UpdateStatusDisplay();
        action Done();
    begin
        (start or UpdateStatusDisplay) where \
            ($TurnsRemaining > 0) => \
                if ( $TurnsRemaining > 0 ) then \
                    TurnsRemaining := $TurnsRemaining - 1; \
                    DoSetBurnRate(); \
                end if;;
        NotifyNewValues => UpdateStatusDisplay();;
        UpdateStatusDisplay where $TurnsRemaining == 0 \
            => Done();;
    end UserInterface;

architecture lander() is
    P1, P2 : Player;
    C : Calculation;
    D : DataStore;
    connect
        P1.DoSetBurnRate to C.SetBurnRate;
        P2.DoSetBurnRate to C.SetBurnRate;
        C.DoSetValues to D.SetValues;
        D.NotifyNewValues to P1.NotifyNewValues();
        D.NotifyNewValues to P2.NotifyNewValues();
    end LunarLander;

```

Such an architecture might be specified as shown in Figure 6-17. This specification begins by defining the types of available component primarily in terms of their interfaces. Each interface has a number of events it can receive and send out ('in' and 'out' actions, respectively). Each component has a behavioral specification as well, defining how it reacts to different events. This simple example takes advantage of only a small number of Rapide language features; it has support for defining and manipulating the data that makes up the events as well. A more complex Lunar Lander specification might actually be able to simulate the entire Lunar Lander game, including data, new state calculations, and so on.

At the end of the specification, the architecture structure is defined: first components that implement the various interface types, and then links between the component interfaces. This Rapide architecture is relatively straightforward: the players start off by sending an updated burn rate — making their first move of the game. Then, they wait for the display to be updated with new status before making another move. Players are limited to three moves in this system so the game does not go into an infinite move (as there is no other end-game condition). The Calculation component waits for a SetBurnRate event. When it receives one, it will fire an internal event, CalcNewState, and then fire a DoSetValues message to the Data Store component to update the game state. When the game state is updated, the Data Store fires a NotifyNewValues event, which causes the players' displays to be updated, thus prompting them to make their next moves.

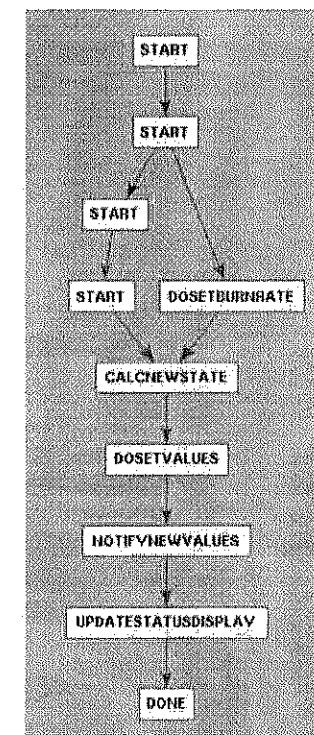
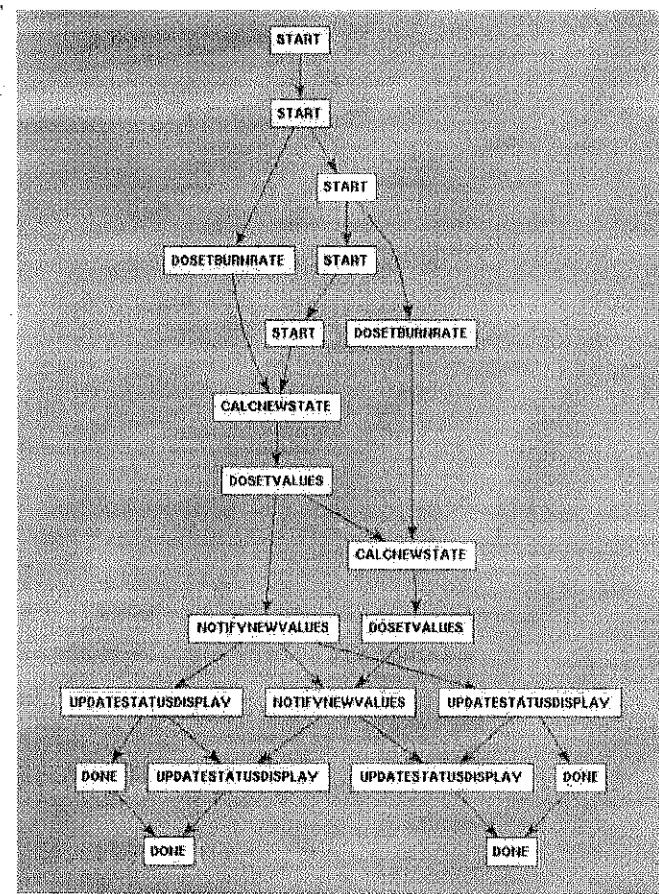


Figure 6-18. Event graph of a one-player Lunar Lander architecture.

In prose, as described here, this implementation strategy might sound perfectly reasonable. But is it? Rapide's analysis and simulation capabilities can help to make that determination. If we remove the second player from the above specification to create only a one-player game and run the Rapide simulator, a graph like the one in Figure 6-18 is generated. The only counterintuitive aspect of this graph is the group of 'start' events that are fired initially. As one of Rapide's primary focus areas is concurrent architectures, it attempts to trigger simultaneous processing by loading the simulation with a number of 'start' events at the beginning. For one player, this version of Lunar Lander looks reasonable.

Figure 6-19. Event graph of a two-player Lunar Lander architecture.



The two-player version of the graph, shown in Figure 6-19, is more complex. This is to be expected. However, by examining the causality arrows, we can see that something is not quite right. The two pathways between the players and the other components are intertwined. Requests are getting intermingled, since there is no locking or transaction support in this design. Furthermore, we can see a fan-out of display updates at the bottom. Each user's display is getting updated twice – once for their own move and once for their partner's. For one turn, this is fine, but recall that

the specification calls for the player to make a move after the display is updated. With more players and more moves come more display updates, and each one will cause a player to try to move, compounding the effect of the interleaving. This is a not-so-obvious bug in the specification: all players should not reactively move after each screen update. Without Rapide's graphs, however, it is not easy to see this. This is the kind of bug that can remain undetected until it is discovered late in development, during implementation or testing, when it is the costliest to fix.

**Takeaways:** Rapide addresses dynamic aspects of architecture directly, and provides tool support for the simulation of those aspects. Stakeholders can directly see how the components in a software system are intended to interact and are dependent upon each other by looking at the results of these simulations. Rapide has several significant drawbacks, however: the notation is arcane, with a steep learning curve, and it lacks support for implementing architectures in a way that is consistent with their specifications.

### Wright

Wright [10] is focused on checking component interactions through their interfaces. Interfaces in Wright are specified using a notation derived from the Communicating Sequential Processes (CSP) formalism [122]. Wright specifications can be translated into CSP, and then analyzed with a CSP analysis tool like FDR [81]. These analyses can determine, for example, if connected interfaces are compatible, and whether the system will deadlock. Additionally, Wright has the ability to specify stylistic constraints as predicates over instances.

### Evaluation Rubric for Wright

<b>Scope and Purpose</b>	Structures, behaviors, and styles of systems that are composed of communicating components and connectors.
<b>Basic Elements</b>	Components, connectors, ports and roles (equivalent to interfaces), attachments, styles.
<b>Style</b>	Supported through predicates over instance models.
<b>Static and Dynamic Aspects</b>	Static structural models are annotated with behavioral specifications that describe how components and connectors should both behave and interact.
<b>Dynamic Modeling</b>	Not available.
<b>Non-Functional Aspects</b>	Not available.
<b>Ambiguity</b>	Wright specifications can be translated into the CSP

	formalism and thus have a formal semantic basis. However, external meaning (e.g., specifically what it means to be a component or a connector) is not specified.
<b>Accuracy</b>	Darwin can be modeled in the formalism known as CSP, which allows the models to be automatically checked for, e.g., structural consistency and deadlock freedom.
<b>Precision</b>	Can describe architecture structures and their behavior in great detail (in fact, formal behavioral specifications are required for analysis).
<b>Viewpoints</b>	Structural viewpoints, behavioral viewpoints, style viewpoints.
<b>View Consistency</b>	Structural and behavioral aspects are intertwined because behavior is specified as a decoration on structural elements. Consistency between style and instances can be automatically determined with a CSP evaluator.

**Lunar Lander in Wright:** The structural aspects of Lunar Lander, modeled in Wright, look similar to depictions we have seen earlier (e.g., in a UML component diagram or Darwin). Wright's distinguishing feature is the CSP-based formal specifications of component/connector interfaces and behavior. These specifications can be specified in a notation that resembles mathematical equations, or an equivalent (if less decorative) ASCII notation. Lunar Lander, specified in Wright, might look like this:

Component DataStore  
 Port *getValues* (*behavior specification*)  
 Port *storeValues* (*behavior specification*)  
 Computation (*behavior specification*)

Component Calculation  
 Port *getValues* (*behavior specification*)  
 Port *storeValues* (*behavior specification*)  
 Port *calculate* (*behavior specification*)  
 Computation (*behavior specification*)

Component UserInterface  
 Port *getValues* (*behavior specification*)  
 Port *calculate* (*behavior specification*)  
 Computation (*behavior specification*)

Connector Call  
 Role Caller = *call* → *return* → *Caller* [] §  
 Role Callee = *call* → *return* → *Callee* [] §

Figure 6-20. Lunar Lander modeled in Wright. Some behavioral specifications are omitted for simplicity but the Call connector is fully specified.

```

    Caller.call → Callee.call → Glue
    Glue = [] Callee.return → Caller.return → Glue
    []\$

Configuration LunarLander
  Instances
    DS : DataStore
    C : Calculation
    UI : UserInterface
    CtoUIgetValues, CtoUIstoreValues, UItoC, UItoDS : Call

  Attachments
    C.getValues as CtoUIgetValues.Caller
    DS.getValues as CtoUIgetValues.Callee

    C.storeValues as CtoUIstoreValues.Caller
    DS.storeValues as CtoUIstoreValues.Callee

    UI.calculate as UItoC.Caller
    C.calculate as UItoC.Callee

    UI.getValues as UItoDS.Caller
    DS.getValues as UItoDS.Callee

End LunarLander.

```

The main thing to notice about this specification is the detailed set of formal specifications of behavior. The CSP formalism, while semantically sound and well-documented, is somewhat arcane and has a steep learning curve that is quite different from learning, for example, a new programming language. The value of these specifications is that properties such as deadlock-freedom can be analyzed, which are difficult or impossible to detect in systems implemented in traditional programming languages.

**Takeaways:** Wright's formal specifications have an extremely high learning curve and cognitive overhead even for the simplest of systems. The analysis capabilities are powerful, but limited to a small set of properties (such as deadlock freedom). However, the extensive formal modeling might be worth the effort in, for example, safety-critical systems. Support for refining architectural specifications into implementations is lacking. Like other early ADLs, Wright is not actively used and supported today.

### 6.5.3 Domain- and Style-Specific ADLs

The ADLs surveyed above are useful for describing software systems in general; they are not bound to or optimized for modeling software systems

in a specific domain or style. However, some ADLs are domain-specific or style-specific, or at least optimized for describing architectures in a particular domain or style.

Domain- and style-specific ADLs are important for several reasons. First, their scope is better tailored to stakeholder needs since it targets a particular group of stakeholders, rather than software and systems developers in general. Second, they are able to leave out unnecessary details and excessively verbose constructs because there is little need for generality. Assumptions about the domain or style can be directly encoded into the ADL's semantics instead of repeated in every model. For example, if a particular style uses the same kind of connector between all components, there is no need to include the notion of a connector in the ADL—the ADL's users and tool-set can just assume that there is a connector between every pair of connected components.

Examples of such ADLs include Koala, Weaves, and AADL. We have discussed Koala previously; it is an ADL used to model families of consumer electronics devices. Weaves is both an architectural style and an associated ADL for modeling systems composed of components that interact through streams of objects. AADL is an industrial ADL tailored for modeling embedded, real-time systems (both hardware and software).

#### Koala

Koala [213] was developed by Philips Electronics to capture the architecture of consumer electronics devices such as televisions, VCRs, and DVD players. It is, to a large extent, a domain-specific ADL—it was developed for the specific use of one company for modeling software in a single domain to address specific issues within that domain. The software systems that Koala models are composed of interconnected software components that communicate via explicit provided and required interfaces.

Semantically and syntactically, Koala is a descendant of Darwin. It uses Darwin's structural concepts of input and output ports, but expands on them through the use of constructs to support product-line architectures. Product lines were introduced earlier, in Chapter 1. Product lines are prevalent in the consumer electronics domain, where a single product like a television may have a host of feature variations: diagonal size, audio/video inputs and outputs, and optional components such as integrated VCRs, DVD players, or both. Separately documenting the software architectures of each of these products would be redundant and error-prone, since substantially the same elements would be repeated over and over again in each product. Koala addresses this by having specific constructs in the language for explicitly defining points of variation. In this way, common elements of the architecture are reused from product to product.

The product-line concepts in Koala will be discussed in detail later in this book, specifically in Chapter 15. We defer the discussion of the specifics of the notation until then; interested readers should skip ahead. The evaluation rubric for Koala is presented here for completeness.

#### Evaluation Rubric for Koala

<b>Scope and Purpose</b>	Capturing the structure, configuration, and interfaces of components in the domain of embedded consumer electronics devices.
<b>Basic Elements</b>	Components, interfaces, and constructs for specifying explicit points of variation: diversity interfaces, switches, and multiplexers.
<b>Style</b>	Koala descriptions capture the architectures of related, variant products simultaneously, and this might be seen as defining a narrow architectural style.
<b>Static and Dynamic Aspects</b>	Only static structure and interfaces are modeled.
<b>Dynamic Modeling</b>	Although points of variation are defined statically in the architecture, the selection of variants could change at runtime.
<b>Non-Functional Aspects</b>	Not explicitly modeled.
<b>Ambiguity</b>	Koala elements are concrete and closely mapped to implementations.
<b>Accuracy</b>	Koala models have well-defined rules and patterns of interconnection. Koala elements are also closely mapped to implementations. Errors in models should be relatively easy to identify by looking for pattern violations or implementation problems like compiler errors.
<b>Precision</b>	The configuration of a system is well-defined in a Koala model, but other aspects of a system are not specified.
<b>Viewpoints</b>	Structural viewpoint with explicit points of variation.
<b>View Consistency</b>	In general, Koala specifications do not include multiple views.

#### Weaves

Weaves [101] is both an architectural style and an accompanying notation. Weaves is used to model systems of communicating small-grain tool fragments that process objects of data. Weaves can be seen as a variant of

the pipe-and-filter style with three significant differences. First, Weaves tools process object streams instead of pipe-and-filter's byte streams. Second, Weaves connectors are explicitly sized object queues, whereas pipe-and-filter connectors are implicit pipes. Weaves connectors serve to facilitate the transfer of both data and control among components. They receive objects from input ports, return control to the calling tool fragment, and then pass the object to tool fragments on output ports in a separate thread of control. Third, Weaves tools can have multiple inputs and outputs, whereas pipe-and-filter components have one input and one output.

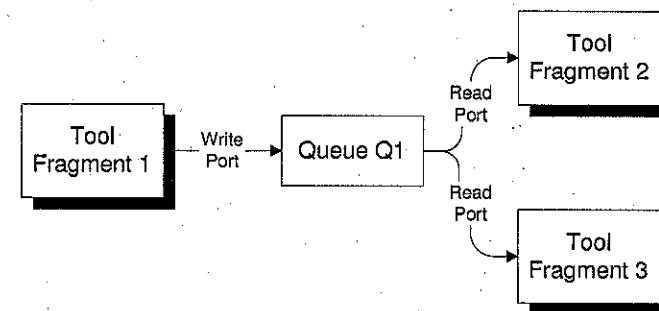


Figure 6-21. A basic weave in the Weaves notation

Figure 6-21 shows a basic architecture expressed in the Weaves notation. The component 'Tool Fragment 1' outputs a stream of objects to an explicit queue connector 'Q1', which forks the stream and forwards the objects to both 'Tool Fragment 2' and 'Tool Fragment 3.' As is obvious from this diagram, the Weaves notation is graphical and minimalist: components are represented by a shadowed box and queue connectors represented by an ordinary box; configurations are expressed using directed arrows connecting components and connectors. Although the Weaves notation is minimal, it is adequate to serve as a description notation for the Weaves style. Weaves reflects an important lesson well-known to architects: perfection is achieved not when there is nothing left to add, but nothing left to take away. In this case, a simple, straightforward notation can be preferable to a complex, inclusive one.

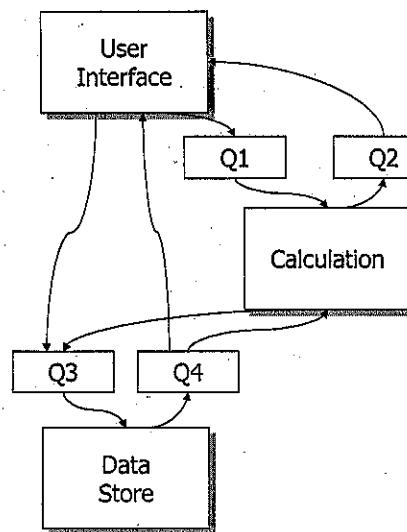
#### Evaluation Rubric for Weaves

<b>Scope and Purpose</b>	The structure and configuration of components in architectures that conform to the Weaves architectural style.
<b>Basic</b>	Components, connectors (queues), and directed

<b>Elements</b>	interconnections.
<b>Style</b>	Weaves models conform to the Weaves architectural style; the constraints of that particular style are implicit in the model.
<b>Static and Dynamic Aspects</b>	Only static structure is modeled.
<b>Dynamic Modeling</b>	Although there is no direct support for dynamic modeling, the Weaves style establishes a close correspondence between components in the architectural model and components in the implementation; changes tracked in one can be straightforwardly applied to the other.
<b>Non-Functional Aspects</b>	The Weaves style induces certain non-functional properties on systems but these are not explicitly modeled.
<b>Ambiguity</b>	The meaning of Weaves elements is well-defined and not ambiguous.
<b>Accuracy</b>	Errors in models are limited to broken links and interconnection problems, which are easy to identify. It should be easily possible to determine whether implementations correspond to Weaves models since there is a close correspondence established by the style.
<b>Precision</b>	The configuration of components and connectors in a system is well-defined in a Weaves model, but other aspects of a system are not specified.
<b>Viewpoints</b>	Structural viewpoint.
<b>View Consistency</b>	In general, Weaves specifications do not include multiple views.

**Lunar Lander In Weaves:** Because Weaves is both a style and an architecture description notation, expressing the Lunar Lander architecture in Weaves means something different than expressing it in a more style-neutral notation like UML or Darwin. The actual models are nearly identical, but even though the models are similar, their meanings are not. Interpreting a Weaves model must be done through the lens of the Weaves architectural style: a component in Weaves is not the same as a component in Darwin. The Lunar Lander system might be expressed in Weaves like this:

Figure 6-22. A  
the Lunar Lander  
application in



Here, the structure of the system itself is directly influenced by the Weaves architectural style. The components here are not communicating by means of request-response procedure calls, but instead through streams of objects. The basic flows of data are similar to the other models depicted above. One notable difference is the explicit presence of return channels for data: in Weaves, the fact that a request travels from the User Interface to the Calculation component (in the above model, through queue Q1) does not imply that a response comes back along the same path. This response's path must be explicitly specified and have its own queue (Q2 in the above model).

Another interesting characteristic of the Weaves model above is that it provides information about structural connections, but does not capture aspects of how those connections are used (e.g., the sequences or protocols of objects that are passed through them). These details could be specified in an additional model, in natural language or a more formal notation. To complete the explanation of the model above, we might include the following specification:

*The connection from User Interface to Calculation (via Q1) carries objects that include a burn-rate and instruct the calculation component to calculate a new Lander state. The connection from Calculation to User Interface (via Q2) indicates when the*

*calculation is complete and also includes the termination state of the application. The connections from User Interface and Calculation to Data Store (via Q3) carry objects that either update or query the state of the Lander. The connections back to User Interface and Calculation from Data Store (via Q4) carry objects that contain the Lander state, and are sent out whenever the state of the Lander is updated.*

**Takeaways:** Weaves shows how binding a notation to a particular style can greatly simplify that notation. Syntactically, Weaves diagrams are extraordinarily simple (even simpler than Darwin diagrams). Unlike Darwin or other general-purpose ADLs, however, the constructs in Weaves diagrams have more specific meanings. The connection from a read port to a write port does not mean just any kind of data or control flow. Rather, it implies a very specific notion of control and data flow involving object streams passed by components running in independent threads of control. When a style is being used, tailored style-specific notations can significantly reduce the cognitive overhead of specifying and interpreting architecture models.

#### The Architecture Analysis and Design Language (AADL)

The Architecture Analysis and Design Language (AADL, formerly the Avionics Architecture Description Language) [73] is an architecture description for specifying system architectures. While its historical name indicates that its initial purpose was for modeling avionics systems, the notation itself is not specifically bound to that domain—instead, it contains useful constructs and capabilities for modeling a wide variety of embedded and real-time systems such as automotive and medical systems. It is an outgrowth of the earlier MetaH architecture description language [19] developed by Honeywell.

Like many of the other ADLs we have surveyed, AADL can describe the structure of a system as an assembly of components, though AADL has special provisions for describing both hardware and software elements, and the allocation of software components to hardware. It can describe interfaces to those components for both the flow of control and data. It can also capture non-functional aspects of components (such as timing, safety, and reliability attributes).

Syntactically, AADL is primarily a textual language, accompanied by a graphical visualization and a UML profile for capturing AADL information in different ways. The syntax of the language is defined using BNF production rules.

The basic structural element in AADL is the component. AADL components are defined in two parts: a component *type* and a component *implementation*. A component type defines the interfaces to a

component—how it will interact with the outside world. A component implementation is an instance of a particular component type. There may be many instances of the same component type. The component implementation defines the component's interior—its internal structure and construction, and so on. One additional element that affects components is a component's *category*. AADL defines a number of categories (or kinds) of components; these can be hardware (e.g., memory, device, processor, bus), software (e.g., data, subprogram, thread, thread group, process), or composite (e.g., system). The category of a component prescribes what kinds of *properties* can be specified about a component or component type. For example, a thread may have a period and a deadline, whereas memory may have a read time, a write time, and a word size.

AADL is supported by an increasing base of tools, including a set of open-source plug-ins for the Eclipse software development environment that provide editing support and import/export capabilities through the extensible markup language (XML) [28]. An additional set of plug-ins is available for analyzing various aspects of AADL specifications—for example, whether all the elements are connected appropriately, whether resource usage by the various components exceeds available resources, and whether end-to-end flow latencies exceed available time parameters.

**Lunar Lander in AADL:** AADL captures the hardware and software elements of a system in great detail, and relates them all to one another. As such, AADL specifications that capture all these elements can become large. Because of this, here we model only a part of the Lunar Lander system: the Calculation component and its connection to the data store component. In this version of Lunar Lander, the two components are connected by a physical Ethernet bus. Also, this is a real-time version of Lunar Lander—instead of operating only when the user inputs a burn rate, the calculation component periodically queries and updates the data store component at regular intervals. Here, perhaps the burn rate is not input from the user at the keyboard, but read at periodic intervals from a sensor connected to a burn-rate knob. This is more consistent with a sense-compute-control architectural style. This part of the Lunar Lander system expressed in AADL might look like this:

```
data lander_state_data
end lander_state_data;

bus lan_bus_type
end lan_bus_type;

bus implementation lan_bus_type.ethernet
properties
  Transmission_Time => 1 ms .. 5 ms;
  Allowed_Message_Size => 1 b .. 1 kb;
```

Figure 6-23. Partial  
Lunar Lander  
specification in AADL

```

end lan_bus_type.ethernet;

system calculation_type
features
    network : requires bus access
        lan_bus.calculation_to_datastore;
    request_get : out event port;
    response_get : in event data port lander_state_data;
    request_store : out event port lander_state_data;
    response_store : in event port;
end calculation_type;

system implementation calculation_type.calculation
subcomponents
    the_calculation_processor :
        processor calculation_processor_type;
    the_calculation_process : process
        calculation_process_type.one_thread;
connections
    bus access network -> the_calculation_processor.network;
    event data port response_get ->
        the_calculation_process.response_get;
    event port the_calculation_process.request_get ->
        request_get;
    event data port response_store ->
        the_calculation_process.response_store;
properties
    Actual_Processor_Binding => reference
        the_calculation_processor applies to
            the_calculation_process;
end calculation_type.calculation;

processor calculation_processor_type
features
    network : requires bus access
        lan_bus.calculation_to_datastore;
end calculation_processor_type;

process calculation_process_type
features
    request_get : out event port;
    response_get : in event data port lander_state_data;
    request_store : out event data port lander_state_data;
    response_store : in event port;
end calculation_process_type;

thread calculation_thread_type
features
    request_get : out event port;
    response_get : in event data port lander_state_data;
    request_store : out event data port lander_state_data;
    response_store : in event port;
properties
    Dispatch_Protocol => periodic;
end calculation_thread_type;

```

```

process implementation calculation_process_type.one_thread
subcomponents
    calculation_thread : thread client_thread_type;
connections
    event data port response_get ->
        calculation_thread.response_get;
    event port calculation_thread.request_get -> request_get;
    event port response_store ->
        calculation_thread.response_store;
    event data port request_store -> request_store;
properties
    Dispatch_Protocol => Periodic;
    Period => 20 ms;
end calculation_process_type.one_thread;

```

The first thing to note about this specification is the level of detail at which the architecture is described. A component (`calculation_type.calculation`) runs on a physical processor (`the_calculation_processor`), which runs a process (`calculation_process_type.one_thread`), which in turn contains a single thread of control (`calculation_thread`), all of which can make two kinds of request-response calls through ports (`request_get/response_get, request_store/response_store`) over an Ethernet bus (`lan_bus_type.ethernet`). Each of these different modeling levels is connected through composition, mapping of ports, and so on. This level of detail emphasizes the importance of tools, such as graphical editors, for modeling this information in a more easily understandable fashion.

The second thing to note about this specification is the use of properties to identify specific characteristics of some of the elements (e.g., the calculation process runs periodically, every 20ms). In a complete system specification, these properties would be even more detailed and elaborate, and could be used to answer questions about availability and timing that are critical in a real-time context.

**Takeaways:** AADL is a high-cost, high-value notation. The syntax and capabilities of AADL are the product of a significant amount of thought and development effort, and the kinds of analyses that can be done on AADL specifications are nontrivial. However, while users leverage the effort of the AADL developers, they also incur their own costs: AADL specifications are complex and extensive, even for small systems. This, in itself, entails significant risks and costs for users. For the specific domain in which AADL is positioned (embedded real-time systems), these costs may be worth it: these systems are often safety-critical and expensive to redeploy. Getting them right the first time is critical.

### 6.5.4 Extensible ADLs

There is a natural tension between the expressiveness of general-purpose modeling languages like UML and the semantic power of more specialized ADLs like Wright, Weaves, and Rapide. On one hand, architects need the ability to model a wide variety of architectural concerns. On the other hand, they need semantically precise languages to reduce ambiguity and increase analyzability. Furthermore, as we have discussed, architectural concerns and product needs can vary widely from project to project. One solution is to use multiple notations, each addressing a different set of architectural concerns. However, this creates difficulty in keeping the different models consistent and establishing traceability between models. Additionally, even using multiple notations, there may be certain concerns that cannot be adequately captured in any existing notation. An approach that addresses these issues is the use of extensible architecture description languages.

Extensible ADLs generally provide a basic set of constructs for describing certain common architectural concerns (e.g., the ability to specify components and connectors). Additionally, they also include support (through the notation and associated tools) for extending the notation's syntax to support new, user-defined constructs. In some cases, the extensions may only modify the existing base constructs. Other notations allow the creation of entirely new constructs and concepts.

The basic approach to employing an extensible ADL is as follows:

1. Determine what concerns can be modeled using the existing (baseline) capabilities of the ADL;
2. For those concerns that cannot be modeled using the baseline capabilities, choose how to extend the ADL to support their modeling (or reuse an extension developed by another user);
3. Extend the ADL and its supporting tools as necessary to support the modeling of the unique features.

Effectively, extensible ADLs can be seen as “domain-specific ADL factories.” Through extension mechanisms, users can tailor these ADLs to meet the needs of their particular domain or project. Examples of extensible ADLs include Acme, ADML, and xADL. Each of these is covered in detail below.

#### Acme

Acme [89] is perhaps the earliest example of an ADL that emphasized extensibility. Acme has a base set of seven constructs: *components* and *connectors*, *ports* and *roles* (roughly equivalent to this book's notion of interfaces on components and connectors, respectively), *attachments* (equivalent to this book's notions of links), *systems* (configurations of

components, connectors, ports, roles, and attachments), and *representations* (inner architectures for components and connectors). These constructs provide a vocabulary for expressing structural design decisions about a system: basically, the system's component and connector makeup in a box-and-arrow form.

Extensibility in Acme is derived entirely through the use of *properties*. Properties are decorations that can be applied to any of the basic seven kinds of elements. Properties are (optionally) typed name-value pairs. Names are simple strings, and the values should conform to the property's type, if it has one. Acme includes a number of simple property types (integers, Booleans, and so on), as well as the ability to use user-defined types. Either way, from Acme's point of view, properties and their values are uninterpreted. It is up to user-written tools to parse these properties (and any internal structure they contain) and do something useful with the contents (e.g., provide analysis or visualization capabilities).

Originally, it was anticipated that Acme's primary use would be as an architecture *interchange* language, rather than an ADL or even an extensible ADL. That is, developers of other ADLs such as Wright and Rapide would develop translators that mapped their languages to and from Acme: in this way, models could be interchanged among many different tools for, e.g., analysis. This strategy was never applied on a wide scale, however, possibly because of semantic differences and conflicts among target ADLs and the limited value added by Acme over simply maintaining multiple concurrent specifications.

#### Evaluation Rubric for Acme

<b>Scope and Purpose</b>	Modeling the structural aspects of a software architecture, with the addition of properties to define other aspects.
<b>Basic Elements</b>	Components, connectors, ports & roles (interfaces), attachments (links), representations (internal structure) and properties.
<b>Style</b>	Stylistic similarities can be modeled through the use of Acme's type system.
<b>Static and Dynamic Aspects</b>	Static structure is modeled natively, dynamic properties can be captured by decorating the static elements with formatted properties.
<b>Dynamic Modeling</b>	A software library, AcmeLib, allows Acme models to be manipulated programmatically.
<b>Non-Functional Aspects</b>	Properties can capture non-functional aspects, but these cannot be automatically analyzed.

Ambiguity	The use of various elements (e.g., components, connectors) is well-defined, but what they mean externally (e.g., what does it mean to be a component) is not defined. In general, Acme properties are not interpreted and can introduce ambiguity if not accompanied by tools or documentation.
Accuracy	The use of various elements (e.g., components, connectors) is well-defined. Typing can be used to check whether elements have particular properties, but external tools are required to check the contents of properties.
Precision	Properties can annotate the existing element types with whatever detail is required, but it is not generally possible to define new kinds of architectural elements.
Viewpoints	Natively, structural viewpoints are supported; properties can be used to provide additional viewpoints.
View Consistency	External tools must be developed to check the consistency of views.

**Lunar Lander in Acme:** The basic specification of Lunar Lander in Acme is similar to models shown above. It is largely structural and includes components, connectors, ports, roles, and attachments. Lunar Lander, specified in Acme, might look like this:

```
//Global Types
Property Type returnsValueType = bool;

Connector Type CallType = {
    Roles { callerRole; calleeRole; },
    Property returnsValue : returnsValueType;
};

System LunarLander = {

    //Components
    Component DataStore = {
        Ports { getValues; storeValues; }
    };
    Component Calculation = {
        Ports { calculate; getValues; storeValues; }
    };
    Component UserInterface = {
        Ports { getValues; calculate; }
    };

    // Connectors
    Connector UserInterfaceToCalculation : CallType {
        Roles { callerRole; calleeRole; },
        Property returnsValue : returnsValueType = true;
    }
}
```

Figure 6-24. Structural Acme model of the Lunar Lander application.

```
Connector UserInterfaceToDataStore : CallType {
    Roles { callerRole; calleeRole; },
    Property returnsValue : returnsValueType = true;
}
Connector CalculationToDataStoreS : CallType {
    Roles { callerRole; calleeRole; },
    Property returnsValue : returnsValueType = false;
}
Connector CalculationToDataStoreG : CallType {
    Roles { callerRole; calleeRole; },
    Property returnsValue : returnsValueType = true;
}

Attachments {
    UserInterface.getValues to
        UserInterfaceToDataStore.callerRole;
    UserInterfaceToDataStore.calleeRole to
        DataStore.getValues;

    UserInterface.getValues to
        UserInterfaceToDataStore.callerRole;
    UserInterfaceToDataStore.calleeRole to
        DataStore.getValues;

    UserInterface.calculate to
        UserInterfaceToCalculation.callerRole;
    UserInterfaceToCalculation.calleeRole to
        Calculation.calculate;

    Calculation.storeValues to
        CalculationToDataStoreS.callerRole;
    CalculationToDataStoreS.calleeRole to
        DataStore.storeValues;

    Calculation.getValues to
        CalculationToDataStoreG.callerRole;
    CalculationToDataStoreG.calleeRole to
        DataStore.getValues;
}
```

One interesting thing to note about this model is its verbosity, especially compared to some earlier models. This is a result of two key decisions made by the Acme designers. First, the Acme language is domain-neutral: little can be abbreviated out of the model, because the underlying Acme semantics make few assumptions about the architecture that allow information to be conveyed implicitly. Second, the Acme designers intended Acme models to be edited through graphical tools, and have also developed an environment called AcmeStudio that allows users to design Acme structures using a GUI interface rather than writing the complete textual description of the model in a text editor. This limits the amount of additional effort Acme users must expend to deal with Acme's verbosity.

A second thing to notice about the model is the use of properties. In this basic model, only one kind of property is used: each procedure call connector is annotated with a property indicating whether the operation has a return value or not. This might be useful to designers looking to make a partially asynchronous version of the Lunar Lander: calls without return values may be able to return control to the caller without waiting for their completion. Acme's type system is used to declare a connector and a property type, such that regularity can be imposed over connectors and properties that are similar (for example, all connectors in the above Lunar Lander model are of the same type: `CallType`). Types in Acme work in a manner similar to stereotypes in a UML profile: they allow the user to set expectations on instance elements that can be checked later.

Compared to the other Lunar Lander models above, this basic Acme model is not very innovative. However, additional properties can add detail to this model in a number of ways, depending on the stakeholder's needs. For example, we might say more about how the *Data Store* component stores its data:

```
Property Type StoreType = enum { file,
    relationalDatabase, objectDatabase };

Component DataStore = {
    Ports {
        getValues; storeValues;
    }
    Property storeType : StoreType =
        relationalDatabase;
    Property tableName : String = "LanderTable";
    Property numReplicas: int = 0;
};
```

Figure 6-25. Extended definition of the Lunar Lander *DataStore* component in Acme

This extended description of the component is intended to indicate that the *DataStore* component should store its data in a non-replicated table called “*LanderTable*” in a relational database. However, the fact that the model uses these particular property names and values is not a standard: tools and stakeholders must be informed about which properties to expect and how to process their values.

**Takeaways:** Notwithstanding the relative failure of architectural interchange, the notion that extensibility should be a primary concern in ADL development is a good one—it is an explicit recognition that there cannot be a *one-size-fits-all* ADL. Property-based decorations as an extensibility mechanism provide a degree of flexibility, but the breadth of architectural concerns that stakeholders want to capture requires the ability to define new first-class constructs.

### The Architecture Description Markup Language (ADML)

The architecture description markup language (ADML) [262] is an XML-based architecture description language whose syntax is derived from Acme. It was originally developed by the Micro-electronics and Computer technology Consortium (MCC) and is an Open Group standard. Semantically, the two are nearly identical, with ADML's primary addition being support for meta-properties. In ADML, meta-properties provide a mechanism by which users can specify what properties (and property types) should be present on particular elements.

Using the extensible markup language, XML, as the basis for an architecture modeling notation confers several benefits. XML provides a standard framework for expressing the syntax of notations. It is well-suited to describing hierarchical organizations of concepts, and internal references can be used to create “pointers” from one element to another. A significant practical benefit of the use of XML is the panoply of off-the-shelf commercial and open-source tools that are available for parsing, manipulating, and visualizing XML documents. Using these tools can significantly reduce the amount of time and effort needed to construct architecture-centric tools like analyzers, editors, and so on.

XML can be used to create languages with extensible syntax. However, early XML standards provided limited support for this. ADML's syntax is defined using an XML document type definition (DTD), one of the earliest XML meta-languages, which uses production rules to define syntax. XML DTDs have been used to create extensible languages, but the mechanisms are somewhat cumbersome. Instead, ADML provides its extensibility through the same mechanism as Acme—name-value pair properties applied to a core set of elements.

**Lunar Lander in ADML:** Because ADML is so similar to Acme, we will not provide a complete ADML description for the Lunar Lander application. The description of the *Data Store* component in ADML might look like this:

```
<Component ID="datastore" name="Data Store">
    <ComponentDescription>
        <ComponentBody>
            <Port ID="getValues" name="getValues"/>
            <Port ID="storeValues" name="storeValues"/>
        </ComponentBody>
    </ComponentDescription>
</Component>
```

Figure 6-26. Description of one Lunar Lander component in ADML

Although the semantic content of this ADML snippet is virtually identical to its Acme counterpart, the use of XML as a standard syntactic

framework opens this specification up to a much wider array of tools like parsers and editors that would not necessarily be otherwise available (or as ubiquitous). One obvious drawback is that by employing XML, the already verbose Acme description has become even more dense. This reflects the overall attitude of XML in general—computing resources and data storage have become inexpensive and plentiful, and editing tools have become ubiquitous. Conservation of data bytes is no longer a driving force in language design.

**Takeaways:** XML provides many extrinsic benefits for architecture modeling, and nearly all architecture description notations still under development at least have the option to import from and export to XML. ADML, however, does not take advantage of one of XML's most powerful features, namely, the extensibility mechanisms.

#### xADL: An Extensible XML-based Architecture Description Language

The architectural concepts that different stakeholders in different domains might want to capture are far too diverse to capture in a single language. Furthermore, while many architecture modeling notations do have certain concepts in common (components, connectors, and so on), these concepts are not adequate to describe every aspect of architecture.

xADL [51] is an attempt to provide a platform upon which common features can be reused from domain to domain and new features can be created and added to the language as first class entities (not just extensions to other entities as with Acme and ADML). Like ADML, xADL is an XML-based language. That is, every xADL model is a well-formed and valid XML document. The main difference is that unlike ADML, xADL fully leverages XML's extensibility mechanisms to support language extensions.

The syntax of the xADL language is defined in a set of XML schemas. XML schemas are similar to DTDs in that they provide a format in which to define the syntax of a language. Whereas DTDs use production rules, however, XML schemas use a data type definition format similar to data structures in an object-oriented programming language. Like classes in an object-oriented programming language, XML schema datatypes can be extended through inheritance. Derived datatypes can be declared in separate schemas. Through this mechanism, datatypes declared in one schema can be extended in a different schema to add new modeling features.

Syntactically, the xADL language is the composition of all the xADL schemas. Each xADL schema adds a set of features to the language. The constructs in each schema may be new top-level constructs or they may be extensions of constructs in other schemas. Breaking up the feature set in this way has several advantages. First, it allows for *incremental*

*adoption*—users can use as few or as many features as makes sense for their domain. Second, it allows for *divergent extension*—users can extend the language in novel, even contradictory ways—to tailor the language for their own purposes. Third, it allows for *feature reuse*—because feature sets are defined in XML schema modules, schemas can be shared among projects that need common features without each group having to develop their own (probably incompatible) representations for common concepts.

From time to time, new schemas are added to xADL as they are developed, both by its creators and outside contributors. Current xADL schemas that will be referenced in this book include:

Schema	Features
<b>Structure &amp; Types</b>	Defines basic structural modeling of prescriptive architectures: components, connectors, interfaces, links, general groups, as well as types for components, connectors, and interfaces.
<b>Instances</b>	Basic structural modeling of descriptive architectures: components, connectors, interfaces, links, general groups.
<b>Abstract Implementation</b>	Mappings from structural element types (component types, connector types) to implementations.
<b>Java Implementation</b>	Mappings from structural element types to Java implementations.
<b>Options</b>	Allows structural elements to be declared optional— included or excluded from an architecture depending on specified conditions.
<b>Variants</b>	Allows structural element types to be declared variant—taking on different concrete types depending on specified conditions.
<b>Versions</b>	Defines version graphs; allows structural element types to be versioned through association with versions in version graphs.

Because xADL can be extended with unforeseen constructs and structures in nearly arbitrary ways, it induces challenges that do not exist in languages with unchanging syntaxes and semantics (i.e., most of the other ADLs we have covered here). Specifically, parsers, editors, analyzers, and other tools must be developed to cope with a notation whose syntax may change from project to project.

xADL addresses these challenges with an associated set of tools that make it easier for users to implement their own tools (e.g., analyzers, editors) that can handle the language's extensible syntax. These are:

**The xADL Data Binding Library:** A data binding library is a software library that provides an API for parsing, reading, writing, and serializing (writing back out to disk or other storage) documents in a particular language. In xADL's case, the data binding library consists of a set of Java classes that can be used to represent xADL elements. There is a one-to-one correspondence between data binding library classes and xADL elements as defined in the xADL schemas. Although xADL documents can be read, written, and manipulated with any XML-aware tool, the data binding library provides a much simpler interface and is the basis for most of the other xADL tools developed to date.

**Apigen:** The data binding library would be of limited use if it had to be manually rewritten each time schemas were added to the xADL. Apigen [53] is a data binding library generator: given a set of XML schemas, it can generate a complete new data binding library with support for those new schemas. Extended data binding libraries can be substituted for existing ones without affecting applications (except to provide support for the new schemas).

The native storage format of xADL is in an XML format. Although XML is designed to be readable by both humans and software tools, certain factors can impede the human-readability of XML documents. Specifically, xADL's extensive use of XML namespaces and multiple schemas adds a significant amount of "housekeeping" data to xADL documents. This data is not without use—it is used by tools such as the data binding library and XML validators—but it makes it more difficult to comprehend a xADL document for humans attempting to read it for content.

For example, a simple component in xADL's XML format might look like this:

```
<types:component xsi:type="types:Component"
    types:id="myComp"
    types:description xsi:type="instance:Description">
    MyComponent
</types:description>
<types:interface xsi:type="types:Interface"
    types:id="iface1">
    <types:description xsi:type="instance:Description">
        Interface
    </types:description>
    <types:direction xsi:type="instance:Direction">
        inout
    </types:direction>
</types:interface>
</types:component>
```

#### Sidebar: xADL and xADL<sub>Lite</sub>

Even with namespace and XML typing information removed, the result is still verbose:

```
<component id="myComp">
    <description>
        MyComponent
    </description>
    <interface id="iface1">
        <description>
            Interface
        </description>
        <directions>
            <inout>
        </direction>
    <interface>
</component>
```

In this book, we will use an alternate representation of xADL documents called xADL<sub>Lite</sub>. xADL<sub>Lite</sub> is a more syntactically terse format than xADL's native XML representation, but the transformation from xADL<sub>Lite</sub> to XML and back again is lossless—no information is lost when translating a document from xADL<sub>Lite</sub> to xADL or back again. Automatic translators are available that can perform the translations. The same component in xADL<sub>Lite</sub> looks like this:

```
component(
    id = "myComp",
    description = "MyComponent",
    interface(
        id = "iface1",
        description = "Interface1",
        direction = "inout"
    )
)
```

#### Evaluation Rubric for xADL

Scope and Purpose	Modeling architecture structure, product lines, and implementations, with support for extensibility
Basic Elements	Components, connectors, interfaces, links, options, variants, versions, plus any basic elements defined in extensions.
Style	Stylistic aspects of an architecture can be modeled through the use of types and type libraries.
Static and Dynamic	Static structure is modeled natively, dynamic properties can be captured through extensions. The MTAT project [117],

Aspects	118] extends xADL to describe the external behavior of components and connectors that communicate through messages.
Dynamic Modeling	The xADL Data Binding Library allows xADL specifications to be manipulated programmatically.
Non-Functional Aspects	Extensions can be written to capture non-functional aspects.
Ambiguity	The xADL language is purposefully permissive in how its elements may be used, although documentation indicates their intended use. Tools are available to automatically check constraints on xADL documents and allow users to define their own constraints.
Accuracy	Tools are provided to check the correctness of xADL documents; additional constraints can be written into these tools to handle extensions.
Precision	Extensions can be used to annotate existing element types with whatever detail is required or create entirely new first-class constructs.
Viewpoints	Natively, structural viewpoints (both run-time and design-time) are supported as well as product-line views; extensions can be used to provide additional viewpoints.
View Consistency	External tools can check the consistency of views; frameworks for developing such tools are provided.

**Lunar Lander in xADL:** For basic structural specifications, xADL has a great deal in common with Acme and ADML. The basic structure of the Lunar Lander application, expressed in xADL's xADLlite textual visualization might look like this:

```
xArch{
    archStructure{
        id = "lunarlander";
        description = "Lunar Lander";
        component{
            id = "datastore";
            description = "Data Store";
            interface{
                id = "datastore.getValues";
                description = "Data Store Get Values Interface";
                direction = "in";
            }
            interface{
                id = "datastore.storeValues";
                description = "Data Store Store Values Interface";
            }
        }
    }
}
```

Figure 6-27. Lunar Lander architecture described in xADLlite

```
        direction = "in";
    }
}
component{
    id = "calculation";
    description = "Calculation";
    interface{
        id = "calculation.getValues";
        description = "Calculation Get Values Interface";
        direction = "out";
    }
    interface{
        id = "calculation.storeValues";
        description = "Calculation Store Values Interface";
        direction = "out";
    }
    interface{
        id = "calculation.calculate";
        description = "Calculation Calculate Interface";
        direction = "in";
    }
}
component{
    id = "userinterface";
    description = "UserInterface";
    interface{
        id = "userinterface.getValues";
        description = "User Interface Get Values Interface";
        direction = "out";
    }
    interface{
        id = "userinterface.calculate";
        description = "User Interface Calculate Interface";
        direction = "out";
    }
}
link{
    id = "calculation-to-datastore-getvalues";
    description = "Calculation to Data Store Get Values";
    point{
        anchorOnInterface{
            type = "simple";
            href = "#calculation.getValues";
        }
    }
    point{
        anchorOnInterface{
            type = "simple";
            href = "#datastore.getValues";
        }
    }
}
link{
    id = "calculation-to-datastore-storevalues";
}
```



doing modeling at all, and significantly better than using a semantically-impoorer notation such as PowerPoint or UML.

Selecting modeling notations is often a subtle activity that involves evaluating multiple characteristics simultaneously—not only what concepts can be modeled, but how they are visualized, what kinds of analyses are available for the notation, traceability to other lifecycle phases, and so on. All these aspects of designing will be addressed in subsequent chapters.

Deciding what to model and what approaches to use is very much a choice driven by costs and benefits. Modeling takes time and effort, as does maintaining models that have already been created. The more complex, precise, and unambiguous the models, the more cognitive effort, time, and money will be invested in creating them.

Different kinds of models produce different kinds of benefits. These benefits generally come in the form of cost mitigation; the models themselves do not produce revenue (except perhaps in the case when they are part of documentation or training that can be sold to customers). Typical benefits of modeling include:

- **As documentation:** Models can serve as points of reference and vehicles for communicating ideas about the system among diverse stakeholders. This increases understanding and reduces confusion, which can lead to fewer problems in later development stages such as integration and acceptance testing. It can also help to determine whether the system is consistent with its requirements and whether the requirements are themselves appropriate.
- **Earlier fault detection:** Good models can help stakeholders detect problems earlier (through inspection and analysis) and fix them before they become costly.
- **Lower change costs:** By giving developers a specific sense of the current architecture (and architectural style), changes can be made following established guidelines with more insight about the effect of a given change on the system.
- **Generation of other artifacts:** Some models can automatically be used to generate specific types of documentation or even (partial) implementations, thus saving the costs of generating these artifacts manually. Generation has the added benefit that it costs less to

#### The Business Case

maintain the connection between models and other development activities, since model changes can simply be used to regenerate other artifacts when they change.

As part of project inception and business planning, it is a good idea to develop a “modeling strategy.” A modeling strategy is simply an agreement between stakeholders on what kinds of models will be constructed, what notations or tools will be used, what consistency criteria will be applied, how those models will be used in the overall development activity, and so on. It is also advisable to develop and document cost/benefit arguments for each model or type of model, capturing the rationale for each model’s creation and use. Additionally, just as project scheduling can be used to estimate the time and cost of implementing various aspects of the system, scheduling can also be applied to the development and maintenance of models.

## 6.8 Review Questions

1. What is an architectural model? What is its relationship to an architecture? To design decisions?
2. What is the difference between accuracy and precision in general? In the context of architectural modeling?
3. What is the difference between a view and a viewpoint?
4. Enumerate some common architectural viewpoints. What kind of data is captured in each viewpoint?
5. What does it mean for two views to be consistent? What kinds of inconsistencies can arise in multi-view models?
6. What kinds of dimensions can you use to evaluate a modeling notation?
7. Enumerate some modeling notations and describe what kinds of design decisions they can capture.
8. What are the distinctive modeling features of Darwin? Of Wright? Of Rapide? Of Weaves?
9. What are the advantages of using an extensible ADL? What are some disadvantages?
10. What are some modeling strategies that can be used when a system is too big or complex to create a complete architectural model?

## 6.9 Exercises

1. Research in more depth the syntax and semantics of one of the ADLs in this chapter and model a system of your choosing in that ADL.
2. Download a tool-set for one of the modeling notations described in this chapter and model a simple application like Lunar Lander in that

- tool-set. Reflect on your experiences and the strengths and weaknesses of the tool-set.
3. Map the syntax of an earlier ADL (e.g., Darwin, Wright, Rapide) to an extensible ADL. What services are provided by the extensible ADL? What extensions are needed to fill in the gaps? Define these extensions using the mechanisms provided by the extensible ADL.
  4. Choose a software-intensive system and research how this system's developers employed modeling. What kind of models were created and how are they used? How are they maintained?
  5. Research how other disciplines (e.g., computer engineering or building architecture) approach the modeling task. What do they model? What notations do they use? Do similar issues (e.g., view consistency) occur in those disciplines? How are they handled there?
  6. Do you agree that UML is an architecture description language? Argue for or against.
  7. Model a simple system like Lunar Lander in two different notations, or in two different viewpoints in the same notation (e.g., two UML diagrams). Ensure that the models are consistent, and explain why and how you established that consistency.
  8. Choose a concern or view not supported by one of the extensible ADLs and develop an extension to support that concern or view.

## 6.10 Further Reading

The chapter opens with an insight about modeling from Maier and Rechtin's *The Art of Systems Architecting* [178]. While not solely about modeling, this book addresses architecture from the perspective of a systems engineer, which is, in general, broader and less concrete than the perspective of a software engineer. As with much of the content of this book, Maier and Rechtin's advice is often equally applicable to both systems and software development.

The bulk of this chapter introduces and surveys a broad variety of modeling notations. Although we have endeavored to distill each notation down to its essence and comment on the aspects of the notations that we feel are distinctive, the few pages dedicated to each notation often cannot adequately capture their scope and subtlety. Interested readers should investigate source documents and specifications related to these notations for more in-depth treatments. Tools for working with unconstrained graphical notations such as PowerPoint [192], Visio [193], and OmniGraffle [281] are widely available. Many books have been written about UML, but the canonical reference is from the developers themselves [24]. Medvidovic and Taylor surveyed early ADLs [189]. These included Darwin [175], Wright [10] (treated even more extensively in Allen's Ph.D. thesis [9]), and Rapide [170], which inspired Luckham et. al.'s later work in complex event processing [168]. UML's takeover of modeling the most generic architectural views resulted in second generation ADLs like Koala

[213] and AADL [73] (itself based on an earlier ADL, MetaH [19]), that addressed more domain-specific concerns. An exciting direction in ADL development remains the creation and growth of extensible ADLs, from early examples like Acme [89] and ADML [262] to later, more flexible examples such as xADL 2.0 [51].

Clements et. al. [38] have dedicated an entire book to the issue of documenting software architectures, which focuses primarily on modeling. Their book takes a viewpoint-centric approach, surveying a wide variety of viewpoints and providing guidance as to what should be captured in each. Their book also surveys salient notations and standards.

## CHAPTER 7

# 7 Visualization

The previous chapter covered modeling: how we ‘write down’ software architectures. To use these models involves reading, writing, and otherwise interacting with architectures. This is where *visualization* comes into play.

**Definition.** An architectural *visualization* defines how architectural models are depicted, and how stakeholders interact with those depictions.

This is an intentionally broad definition of visualization. Here, visualization consists of two key aspects: *depiction* and *interaction*. Put simply, a *depiction* is a picture or visual representation of architectural design decisions in a particular format. A visualization may also provide one or more *interaction* mechanisms through which users can interact with those decisions in terms of the depiction. These mechanisms may include keyboard commands, point-and-click operations, and so on.

This chapter will discuss the relationship between architecture modeling notations and visualizations, and how various modeling languages are visualized. It will then cover various strategies for designing and evaluating visualizations to maximize their effectiveness. The chapter will conclude with a survey of various visualization techniques and evaluations of the strengths and weaknesses of each technique.

This chapter is not intended to be a treatment of techniques for usability design or information visualization in general; these subjects are too broad for the scope of this book. Instead, the chapter will focus on identifying the kinds of visualizations that can be used for architectural models, as well as to discuss issues specifically related to visualization of architectures.

7 Visualization
7.1 Visualization Concepts
7.1.1 Canonical Visualizations

- 7.1.2 Textual Visualizations
- 7.1.3 Graphical Visualizations
- 7.1.4 Hybrid Visualizations
- 7.1.5 The Relationship between Visualizations and Views
- 7.2 Evaluating Visualizations
- 7.2.2 Constructing a Visualization
- 7.2.3 Coordinating Visualizations
- 7.2.4 Beyond Design: Using Visualization Dynamically
- 7.3 Common Issues in Visualization
- 7.3.1 Same Symbol, Different Meaning
- 7.3.2 Differences without Meaning
- 7.3.3 Decorations without Meaning
- 7.3.4 Borrowed Symbol, Different Meaning
- 7.4 Evaluating Visualization Techniques
- 7.5 Techniques
- 7.5.1 Textual Visualizations
- 7.5.2 PowerPoint-like
- 7.5.3 UML: The Unified Modeling Language
- 7.5.4 Rapide
- 7.5.5 The Labeled Transition State Analyzer (LTSAN)
- 7.5.6 xADL 2.0
- 7.6 End Matter
- 7.7 Review Questions
- 7.8 Exercises
- 7.9 Further Reading

## 7.1 Visualization Concepts

Visualization plays a critical role in software architecture. An important concept for this chapter is that the way architectures are *visualized* does not necessarily have to be directly connected to how they are *modeled*. The two are closely related; in fact, each modeling notation is associated with one or more canonical or “native” visualizations (this will be discussed in more detail below). Fundamentally, however, a *model is just information*. It is a set of design decisions. Visualizations are the means by which these design decisions are given form: how they are depicted and how users interact with them.

A single architectural model can be visualized in any number of ways, and multiple diverse models can be visualized in similar ways. Thus, visualization can be used to “hide” (or at least ‘smooth over’) differences in back-end modeling notations. Second, visualizations can vary widely—many are graphical, but most ADLs have textual visualizations as well. Research has even been done in the area of esoteric visualizations, such as three-dimensional models in virtual realities [72].

The goal of this section is to distinguish visualizations from their underlying modeling notations, introduce the kinds of visualizations that can be used to model architectures (textual, graphical, and hybrid), and then discuss the issues that arise when multiple visualizations (of all these kinds) are simultaneously applied to an architecture.

### 7.1.1 Canonical Visualizations

No modeling notation is completely divorced from visualization. Every notation has at least one visualization that is directly and specifically associated with the notation. Notations with multiple views are often associated with multiple canonical visualizations—one per view; views will be covered in the next section.

Text-based ADLs (including XML-based ADLs) are natively expressed using text-based visualizations. Not all modeling notations are textual, however. PowerPoint and Visio models, for example, are manipulated entirely in graphical visualizations, and there is no easy way to extract a text-based representation of the model. UML is a notation whose native visualizations are partially graphical and partially textual. UML diagrams are primarily graphical. The types of elements in the diagrams are defined by UML's metamodel, but their specific graphical look of various elements (classes, statechart nodes, and so on) is actually defined in other documentation. Some parts of UML, such as the OCL constraints that are used to constrain relationships between model elements, are textual, having a well-defined syntax and semantics all their own.

A common pitfall is for users to associate an architecture modeling notation *only* with its canonical visualization, or to view a notation and its canonical visualization as *the same thing*. They are not: the notation is a way of organizing (abstract) information, and the visualization dictates how the information is *depicted* and *interacted with*. For example, most tools that deal with architectural models store the model in data structures in memory, associated with no specific visualization; it is not until an editor is invoked that this information is visualized. Canonical visualizations often present the information in a way that is closely related to its organization, but remember that this is almost always not the only way to present the information.

Not all visualizations are optimal for all uses, and notations that provide multiple visualizations are generally preferable to those that include only one. Furthermore, it may be easier to develop a new visualization for an existing notation than to develop an entirely new notation to underlie a desired visualization.

### 7.1.2 Textual Visualizations

Textual visualizations depict architectures using ordinary text files. These text files generally conform to a particular syntactic format, much like a .c or .java file conforms to the syntax of the C or Java language. (As we have discussed, architectural decisions can also be documented using natural language, in which case the textual visualization would only be constrained by the grammar and spelling rules of that language).

```

<instance:xArch xsi:type="instance:XArch">
  <types:archStructure xsi:type="types:ArchStructure"
    types:id="ClientArch">
    <types:description xsi:type="instance:Description">
      Client Architecture
    </types:description>
    <types:component xsi:type="types:Component"
      types:id="WebBrowser">
      <types:description xsi:type="instance:Description">
        Web Browser
      </types:description>
      <types:interface xsi:type="types:Interface"
        types:id="WebBrowserInterface">
        <types:description xsi:type="instance:Description">
          Web Browser Interface
        </types:description>
        <types:direction xsi:type="instance:Direction">
          inout
        </types:direction>
      </types:interface>
    </types:component>
  </types:archStructure>
</instance:xArch>

xArch{
  archStructure{
    id = "ClientArch"
    description = "Client Architecture"
    component{
      id = "WB"
      description = "Web Browser"
      interface{
        id = "WebBrowser"
        description = "Web Browser Interface"
        direction = "inout"
      }
    }
}

```

Figure 7-1 shows two textual depictions of the architecture of a Web client consisting of only one component: a Web browser. The first depiction depicts an architecture in xADL's native XML format, and the second

depicts the same exact architecture in xADL<sub>Lite</sub>. This is an example of different visualizations being applied to the same model. The XML visualization of the architecture is easily read, manipulated, and syntactically validated by XML tools. The xADL<sub>Lite</sub> visualization describes the same architecture (and is in fact directly derived from the same model), but is better optimized for human read- and writeability.

Textual visualizations have several advantages. They generally depict the entirety of an architecture in a particular notation in a single file. Hundreds of text editors are readily available that allow the user to interact with text files. Years of research has gone into technologies for parsing, processing, and editing structured text files. When a textual syntax is defined using a meta-language such as Backus-Naur Form (BNF), a plethora of tools is available to generate program libraries that can parse and check the syntax of text documents written in that language. Many text editors provide additional developer support for particular notations with features such as auto-complete and syntax checking as-you-type.

Textual notations have disadvantages, as well: textual notations are good at depicting data linearly and hierarchically (think of a program in a language like C or Java: linear ordering is done using lines from top-to-bottom, and hierarchical structure is captured using indentation).

However, graphlike structures and data that benefits from distinct spatial relationships in presentation are not easily understood (by people) through a textual visualization. Additionally, textual visualizations are generally limited to showing a contiguous screenful of text, with few options to organize the text differently (although some advanced environments may include features such as ‘code folding’ that allow users to collapse a block of text into a single line).

### 7.1.3 Graphical Visualizations

Graphical visualizations depict architectures (primarily) using graphical symbols instead of text. Like textual visualizations, graphical visualizations generally conform to a syntax (this time of symbols instead of text elements), but they may also be free-form ('high-level' or 'overview' diagrams of architectures are often free-form and stylistic).

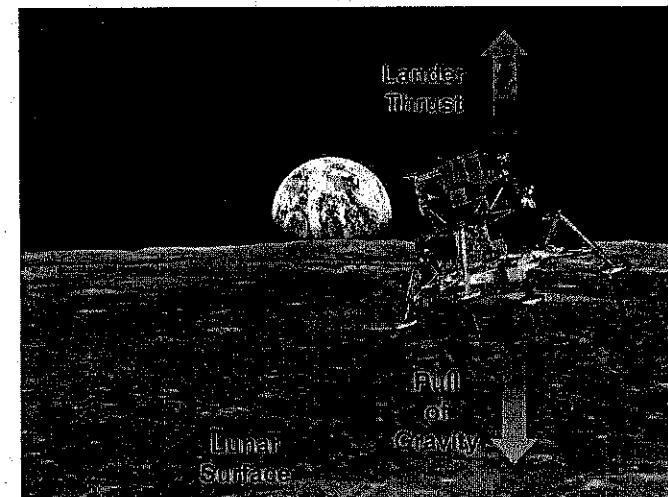


Figure 7-2. Two graphical visualizations of the same architecture

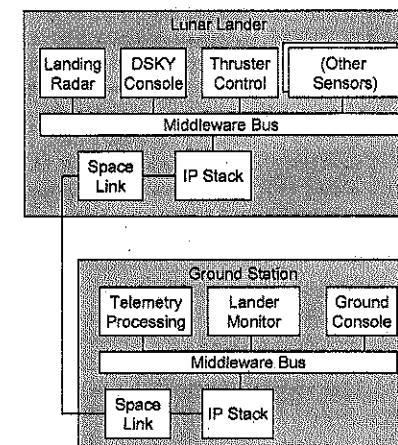


Figure 7-2 shows two graphical depictions of the Lunar Lander architecture. The top depiction is a high-level overview of the Lander and its mission. While this depiction lacks rigor or formality, it does convey useful information to stakeholders that are encountering the application for the first time. Such depictions are often used as conceptual overviews of

complex applications, especially those consisting of many interconnected systems. Standards such as the Department of Defense Architecture Framework (DoDAF, discussed more extensively in Chapter 16) include such depictions—this depiction would satisfy the DoDAF “OV-1” view of the Lunar Lander architecture [67]. Note, however, that it is ambiguous or misleading in several important ways: for example, the Lander is tilted somewhat with respect to the moon’s surface, which may imply a 2- or 3-dimensional aspect to the game that does not exist in the final application. It also depicts the Earth in the background, which may lead one to believe that communications from Earth play a role in the Lander simulation.

The bottom depiction is a logical view of the Lunar Lander architecture, depicting its structure in terms of a component and connector graph. This view is more rigorous, less ambiguous and depicts more information at the cost of being less accessible to outside stakeholders. The overall mission and purpose of the system is lost in the detail of the components and their interconnections.

Graphical visualizations give stakeholders access to information about an architecture in many ways that textual visualizations cannot. Symbols, colors, and other visual decorations can generally be distinguished more easily than elements of structured text. Non-hierarchical relationships between elements can be seen much more easily in a graph than a text file. Graphical visualizations can use spatial relationships to express relationships among elements. Advanced graphical visualizations may also employ animation or other visual effects to highlight or demonstrate different aspects of architecture. Options for interacting with graphical visualizations are generally superior to text visualizations, as well: scrolling, zooming, “drilling down,” showing and hiding different levels of detail, and direct manipulation of objects with the mouse are all commonplace in graphical visualizations. For example, a graphical environment might allow a user to connect components by simply drawing a line between their interfaces with the mouse.

A major disadvantage of graphical visualizations is the cost of building tools to support them. Many tools exist for creating graphical diagrams—PowerPoint, Visio, OmniGraffle, Photoshop, and Illustrator are a few of the more popular ones. However, these tools lack understanding of architectural semantics, and it is difficult (and sometimes impossible) to add appropriate semantics and interaction operations to these tools so they can be integrated into a wider software engineering environment. Furthermore, these tools generally have their own (usually proprietary) file formats and in-memory models that are difficult to connect to a more architecture-centric representation [98] [241].

### 7.1.4 Hybrid Visualizations

‘Graphical’ and ‘textual’ are rough ways of categorizing visualizations. However, many visualizations blur the line between these categories. Few graphical visualizations use only symbols—generally, text is used to decorate, label, or explain the meaning of various elements. Some visualizations go even further, expressing some kinds of design decisions using graphics and others using text. For example, a UML class diagram is primarily composed of interconnected symbols, but constraints on relationships between the symbols are depicted in the object constraint language (OCL) with an exclusively textual visualization.

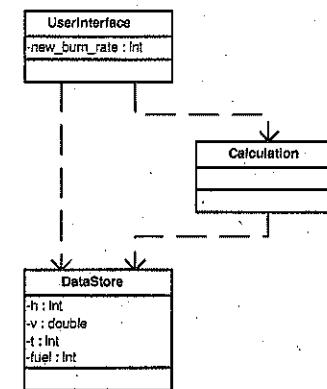


Figure 7-3. UML with constraints as a hybrid visualization.

context UserInterface  
Inv: new\_burn\_rate >= 0

Figure 7-3 depicts UML as a hybrid visualization. The class diagram is primarily graphical, capturing the three primary Lunar Lander elements—user interface, calculation, and data store. Alongside the class diagram, textual OCL is employed to depict the constraint that the new burn rate must be non-negative.

Some visualizations can be composites of many different visualizations, both graphical and textual. For example, the UML composite structure diagram is a primarily graphical visualization used to contain other UML diagrams. Such composite visualizations can be good for displaying relationships between different aspects of the same architecture. Composite visualizations can become complex and confusing quickly as different depiction and interaction mechanisms are combined. Strategies such as ‘drill-down’ interaction mechanisms, where users can navigate to

sub-visualizations from a higher-level composite visualization, can mitigate this complexity.

### 7.1.5 The Relationship between Visualizations and Views

Some visualizations may depict the whole architectural model at once, but more often different visualizations are used to depict different views of the architecture. The last chapter presented the concept of views: subsets of the architecture—usually organized around a single concern or set of concerns. Recall the definitions we presented:

**Definition:** A *view* is a set of design decisions related by a common concern (or set of concerns).

**Definition:** A *viewpoint* defines the perspective from which a view is taken.

Effectively, views and viewpoints let us consider different subsets of the design decisions in an architecture. We can apply the same concept of a subset to visualizations: a visualization for a viewpoint defines depiction and interaction mechanisms only for the kinds of design decisions included in that viewpoint. We associate visualizations with viewpoints rather than views because the same visualization can be used to visualize many different architectures: we do not create a new visualization for every architecture. For example, the UML class diagram is a visualization that can be used to visualize the class structure of many different applications. Two different class diagrams are not two separate visualizations, they are simply two instances of the ‘UML class diagram’ visualization.

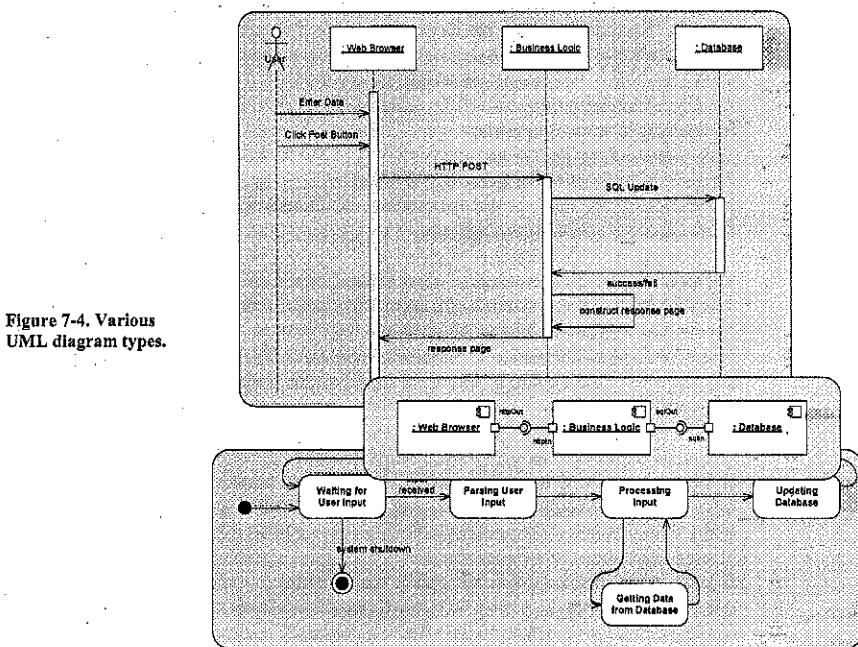


Figure 7-4. Various UML diagram types.

When a notation is associated with a set of viewpoints, it is often the case that each viewpoint has its own canonical visualization. UML is a good example of this: each UML diagram can be seen as a visualization of one particular view of the described system’s architecture. Although UML’s canonical visualizations are all graphical, they differ widely: the box-and-arrow style diagram used to depict components and their relationships bears little resemblance to the automata-like statechart or timeline-like sequence diagrams, as seen in Figure 7-4. This is a natural consequence of the fact that architecture models capture a wide variety of information about a system. What constitutes a useful visualization for one concern may be useless for another concern. Just as system stakeholders should identify the viewpoints they will use to examine and work with an architecture, they should also identify appropriate visualizations for each viewpoint.

All our earlier comments about the relationship between visualizations and models apply equally to partial models—that is, views. Just as multiple visualizations can be applied to the same model, multiple visualizations

can also be applied to the same partial model (view). If the same subset of the architecture is simply presented in two different ways, these are *not* two different views of the architecture: these are two different visualizations of the same view.

In Chapter 6, we showed a depiction of Lunar Lander in xADL, followed by the equivalent depiction in Archipelago.

```
xArch{
    archStructure{
        id = "lunarlander";
        description = "Lunar Lander";
        component{
            id = "datastore";
            description = "Data Store";
            interface{
                id = "datastore.getValues";
                description = "Data Store Get Values Interface";
                direction = "in";
            }
            interface{
                id = "datastore.storeValues";
                description = "Data Store Store Values Interface";
                direction = "in";
            }
        }
    }
}
```

**Figure 7-5.** Lunar Lander in two different visualizations: a xADL textual visualization (abbreviated for space) and an Archipelago visualization.

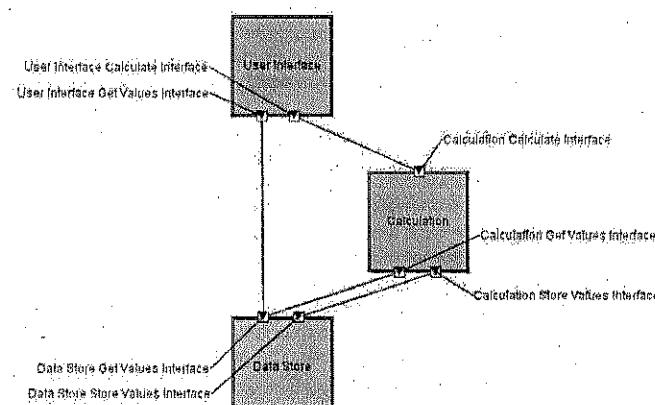


Figure 7-5 repeats the two depictions from Chapter 6 (although the extensive xADL visualization has been abbreviated). This is an example of two different visualizations for the structural viewpoint being applied to the same subset of design decisions (i.e., view) of the Lunar Lander architecture.

## 7.2 Evaluating Visualizations

The above sections outlined what visualizations are, what kinds of visualizations exist, and the relationships between visualizations, models, views, and viewpoints. However, a key question now emerges: what makes a visualization “good”? How can one distinguish visualizations from one another, and choose the best one? Ultimately, the worth of a visualization is dependent upon how well it fits the needs of a project’s stakeholders. As we have seen, stakeholder needs and priorities vary from project to project, so a visualization that is perfect for one project may be useless in another. Nonetheless, it is possible to identify some desirable qualities for visualizations, which can be prioritized by stakeholders to fit specific situations. These qualities include:

### Fidelity

*Fidelity* is a measure of how faithful the visualization is to the underlying model and modeling notation. In general, the minimum acceptable fidelity for a visualization requires that information in the visualization be consistent with the underlying model. It would be extremely confusing, for example, if a structural visualization showed components that were not actually in the architecture, and so on. However, visualizations do not have to address *all* the information in an underlying model. Leaving some detail out can often make visualizations more effective by focusing attention on the parts of the model that matter in a given situation. Such is the case for visualizations that are associated with particular viewpoints, for example.

Fidelity affects both depiction and interaction. An interaction mechanism is faithful if it respects the underlying syntax and semantics of the visualized notation. For example, an interface that allows stakeholders to change the model in invalid ways may be confusing. A balance must be struck between fidelity and usability: preventing users from making mistakes limits exploratory design.

### Consistency

*Consistency* is a measure of how well a visualization uses similar depictions and interaction mechanisms for similar concepts. This sense is one of internal consistency (whether a visualization is consistent with itself) rather than consistency with the underlying model (which we call fidelity). In terms of depiction, consistent visualizations display similar concepts in similar ways. For example, in UML, an object is always

depicted as a rectangle with an underlined name no matter what context it appears in. UML is not perfectly visually consistent, however: in most diagrams, a dashed open-headed arrow represents a dependency, whereas in a sequence diagram, it represents an asynchronous invocation or message. In terms of interaction, consistent visualizations permit the user to do similar things in similar ways. If double-clicking on one element allows the user to assign a name to that element, requiring the user to right-click and select a menu option to assign a name to another kind of element would be inconsistent.

In general, more consistent visualizations are preferable to less consistent ones. The exception once again occurs at the extremes: being too consistent might cause a visualization to have a huge and confusing variety of symbols (to make sure no two concepts share a symbol) or limit the conciseness of a visualization.

#### **Comprehensibility**

*Comprehensibility* is a measure of how easy it is for stakeholders to understand and use a visualization. This makes comprehensibility a function of both the visualization and the stakeholders who use it. Many factors contribute to comprehensibility, including the complexity of the visualization and how information is presented, the complexity of the interaction interface and the skill-sets and prior experiences of the stakeholders.

One way to improve comprehensibility is to narrow the scope of a visualization, limiting the number of concepts it tries to capture and optimizing the visualization to capture only these concepts. Trying to display too much information at once—or many unrelated concepts simultaneously—complicates a visualization and increases its complexity. Alternatively, the comprehensibility of a visualization can be improved by leveraging stakeholder knowledge. For example, using a UML ‘component’ symbol to represent components in non-UML diagrams can make a visualization more comprehensible to stakeholders that already have experience with UML. (Of course, this can backfire if stakeholders bring along assumptions about UML components that are not being implied by the use of the symbol).

#### **Dynamism**

*Dynamism* is a measure of how well a visualization supports models that change over time—in Chapter 6 these are referred to as *dynamic models*. Information about changes flows two ways: changes to the model (from whatever source) can be reflected in the visualization, and changes to the visualization (through one of the interaction mechanisms) can be reflected in the model.

A range of possibilities exists here. An ideal dynamic visualization will be immediately updated when the underlying model changes from any source. Additionally, changes to the visualization through interaction mechanisms should cause the model to be updated accordingly.

In general, the depiction of a dynamic model will involve some kind of asynchronous animation; otherwise, the visualization will become inconsistent as the model changes. A less desirable alternative is to allow the user to manually refresh the visualization, optionally notifying the user when the underlying model has changed so that they can perform a refresh operation. With respect to interaction, any visualization that allows editing must be, to some extent, dynamic. Visualizations that update the underlying model in real-time, as the user works, are generally preferable to those that only store changes periodically, or at the user’s request through, for example, a ‘save’ operation.

#### **View Coordination**

*View coordination* is how well one visualization is (or can be) coordinated with others. In general, environments that allow multiple visualizations to be presented and used simultaneously give users more insight and capability when designing or reviewing an architecture. However, coordinating multiple visualizations is not always straightforward or easy. Strategies for coordinating visualizations are discussed in their own section below.

#### **Aesthetics**

*Aesthetics* is a measure of how pleasing a visualization is to its users. Aesthetics is not limited to depiction; user interfaces have aesthetic qualities as well. Here, depiction is the ‘look’ and interaction is the ‘feel’ of the visualization. Compared to other qualities, aesthetic qualities are extremely subjective. However, there is an enormous amount of literature available on evaluating and designing aesthetically pleasing displays of information. This comes from both the computer science community (e.g., user interface design) and from other communities (art, advertising, marketing, etc.) For example, color theory is instructive in choosing attractive and complementary colors for graphical visualizations; determining which colors are complementary is easy with a color wheel and some basic knowledge of how color schemes are constructed, and nearly impossible using intuition alone.

Technologists have a tendency to ignore or de-prioritize aesthetic aspects of visualizations because they generally add little functional value. However, aesthetic qualities can often make the difference between a visualization being accepted or rejected by potential users.

### Extensibility

*Extensibility* is a measure of how easy it is to modify a visualization to take on new capabilities, either of depiction or interaction. Just as underlying models and notations are often extended to support domain- and project-specific goals, visualizations of those models must be extended as well. A visualization that is difficult or impossible to extend will become less and less useful as underlying models expand to take on new concepts.

Mechanisms to support extensible visualizations include plug-in APIs, scripting support, and even simply open-sourcing the code that implements the visualization so others can modify it.

### 7.2.2 Constructing a Visualization

By now, it should be clear that the kinds of concepts that can be captured in an architecture are diverse and complex. They range from structural components and connectors to their interfaces to the schedules according to which they will be developed. Stakeholders choosing to include these elements in their architectures will also have to choose how they are depicted and manipulated in various visualizations.

If a pre-existing or off-the-shelf notation is used to capture the architecture, its canonical visualizations will be available. For example, UML captures the notion of a class and has a specific symbol used to depict that class.

When decisions and elements are captured that do not have a canonical visualization, or the canonical visualization is insufficient or inadequate, stakeholders have the option of constructing new visualizations. Creating "good" visualizations is somewhat of an art form, but there are a few things to consider:

**Borrow elements from similar visualizations:** Even if you choose not to use UML to capture your architecture, it may be valuable to borrow certain symbols or conventions from UML: the shape of a package symbol to depict one of your packages, or the closed white headed arrow to depict a generalization relationship. This has the advantage that many users will already be familiar with the depiction and its meaning. However, there are also drawbacks: users may assume that your diagrams *are* UML (when they are not), or they may assume specific semantics that you did not mean to import when you used the symbol. A good source for generic symbols that do not carry extensive semantic implications is flowcharting. Although flowcharts have fallen further and further into disuse as programs become more complex, they are still well-understood by a wide variety of users. Common flowcharting symbols useful outside the context

of flowcharts include the diamond (decision point), the vertical drum (disk storage), the sideways drum (memory storage), and so on.

**Be consistent among visualizations:** If you are depicting the same concept in many visualizations, use similar symbology. Likewise, try to avoid using the same symbology to depict different concepts in different visualizations.

**Give meaning to each visual aspect of elements:** In a diagram depicting a graph of many components, it is tempting to depict components with different colors simply to prevent the diagram from looking too monochromatic, without further reason. While this may be aesthetically pleasant, it is confusing from a semantic perspective, since the visual aspect of color has no relationship with the underlying architectural model. It is a good idea to use visual decorations, but each decoration should have precise meaning.

On a related note, users have a tendency to (often subconsciously) embed real semantic information in visual decorations without making that information explicit in the architectural model. For example, in a box-and-arrow graph depiction, a user might place components close to one another to indicate that they share functionality or arrange the components in a layered fashion to reflect an implicit understanding that there are layer-like dependencies in the architecture. When this occurs (and the relationships are not formally documented), valuable information becomes embedded and lost in the visualization. Here, stakeholders should consider whether these visual relationships have semantic importance and, if so, find a way to include them explicitly in the system's models.

**Document the meaning of visualizations:** While we would all like to think that our diagrams and other visualizations are self-explanatory, this is generally not the case. Documenting what each aspect of the diagram means, using a legend, design document, or organizational standard is key to reduce confusion among stakeholders. At best, each aspect of the visualization should correspond to a piece of information in the model.

**Balance traditional and innovative interfaces:** It is fair to assume that most stakeholders involved in software design will have used a significant amount of software themselves. As we have pointed out, 'borrowing' well-known depiction and interaction techniques allows users to leverage their previous experience. However, adhering too closely to this guideline will result in stagnant visualization design. From time to time, consider borrowing useful non-traditional and innovative visualization features as well, or even developing one's own.

For example, most users will assume that a box-and-arrow graph visualization for an architecture's structure will look and work like that of PowerPoint or Visio. However, it is almost certainly not the case that PowerPoint and Visio have perfected box-and-arrow graph editing. Here, one could consider advanced layout paradigms like fisheye layouts, where information is displayed at large sizes in the center of the display and at smaller sizes at the edges, or drill-down paradigms, where zooming in is used as a visual metaphor for looking at more detailed information. A good source of inspiration in visualization design is other software packages that are outside the realm of software design: CAD applications, video games, and so on. Aspiring visualization designers should take note of unusual but useful user interfaces that they encounter and determine how to apply those design ideas to architecture visualization.

Edward Tufte is a Professor Emeritus of statistics, information design, interface design, and political economy at Yale University. He is best known for a series of influential books, including *The Visual Display of Quantitative Information* [293] and *Envisioning Information* [292], that offer practical advice on how to visualize complex data sets to maximize impact and effectiveness. While Tufte's work focuses primarily on static depictions of statistical and quantitative data, many of his lessons can be useful in the design and evaluation of software architecture visualizations as well.

Tufte's approach can be summarized as one of parsimony. A core concept in Tufte's work is maximizing the *data-ink ratio*—designing depictions that focus on depicting the target data and interpretation aids with as few distractions, decorations, or embellishments as possible. He coined the term "chartjunk" to refer to such elements that detract from the display of data. Chartjunk may be obvious—the use of meaningless colors, shadows, photographic or textured fills, and so on. Chartjunk can also be subtle—excessively bold grid lines in a background, thick borders around data elements that diminish the perceived importance of the data, and so on. For Tufte, graphical depictions are not always ideal: simple textual organizations of data (primarily tables) can often convey the same information with far less "ink" and far fewer distractions.

Tufte's advocacy of parsimony does not necessarily equate to minimalism, however. Many of Tufte's examples, particularly where complex data sets are used, are extraordinarily dense and display multiple properties of the data simultaneously. Nonetheless, these depictions still focus strongly on the data itself. *Envisioning Information* in particular delves into issues related to the display of such data sets.

In *Envisioning Information*, Tufte generally advocates increasing the

#### Sidebar: Applying Edward Tufte's Lessons to Software Architecture Visualization

dimensionality of representations as a way to deal with complex data. In this book, Tufte opens by lamenting the limitations of "flatland"—the two-dimensional space provided by pieces of paper and computer screens. He presents several different strategies for breaking out of "flatland," primarily through integrating additional spatial or temporal dimensions into depictions. In a two-dimensional medium, perspective can be used to create three-dimensional spatial pictures. At the time of the book's publication in 1990, 3D rendering technologies were still somewhat inaccessible, and many examples in the book show 3D depictions hand-drawn by artists, although a few simple computer-generated 3D graphs appear as well. Another way to add spatial dimensions to "flatland" is through layering: breaking up the data into multiple depictions that are combined or overlaid on one another. Temporal dimensions can also be taken into account by showing the same data several times in different states, representing different "snapshots" in time. Spatial and temporal dimensions can be added through a concept Tufte calls "small multiples"—showing many small, simple depictions of related data (or the same data at different times) next to each other in succession, making it easy for readers to compare at a glance.

These techniques (three-dimensional depictions, layering, time variation, and small multiples) can all be applied to the construction of software architecture visualizations, although it is certainly the case that few visualizations take advantage of them today. This also represents an area of ongoing research; for example, the EASEL project [119] is focused on bringing interactive layering concepts to a xADL-based architecture development environment.

Tufte's work focuses primarily on static depictions of information. However, a new set of possibilities opens up when the interactivity of a computer is brought to bear. Computers, particularly modern PCs with fast processors, high-resolution color displays, and specialized graphics hardware, can be used to create interactive visualizations that provide an even more immersive escape from "flatland." Although still confined to a fundamentally two-dimensional screen, three-dimensional rendering technology is now available to everyone, and three-dimensional depictions no longer have to remain fixed on a page. A user can easily take a 3D model and rotate, examine, and manipulate it in virtual space from any angle using a computer. To date, 3D views of software architectures have not yet made a mainstream impact. This may be because they are not mature enough yet, or it may be that they are simply not useful for depicting the kind of data that comprises an architectural model. Projects like EASEL, cited above, not only break down architectures into layers, but allow live interaction with those layers, turning them on and off, using them to express alternatives, and so on. Animation has been used in

limited ways to provide a temporal dimension to architectural visualizations (usually effect visualizations that result from some sort of simulation) but far more work needs to be done here as well.

Tufte and the designers of architecture visualizations have much to learn from each other. Tufte's work provides valuable insights on depicting information far more complex than the average architectural model in a very limited medium (static two-dimensional paper). Even with these restrictions—and perhaps because of them—he advocates exploiting dimensions that are still not well-utilized by modern architecture visualizations. On the other hand, architectural visualizations, especially those implemented in an editor or other tool, can exploit the resources of fast computers with high-resolution displays to create much more dynamic visualizations than are possible on paper. Those wishing to design new visualizations (or evaluate existing ones) would do well to absorb Tufte's lessons and contextualize them in terms of an interactive computer-based medium.

### 7.2.3 Coordinating Visualizations

When multiple visualizations of the same information are available, it is key to coordinate these visualizations with each other, so that changes to the information via one visualization are accurately reflected in other visualizations. If the visualizations are not coordinated, they can become out-of-sync and cause confusion.

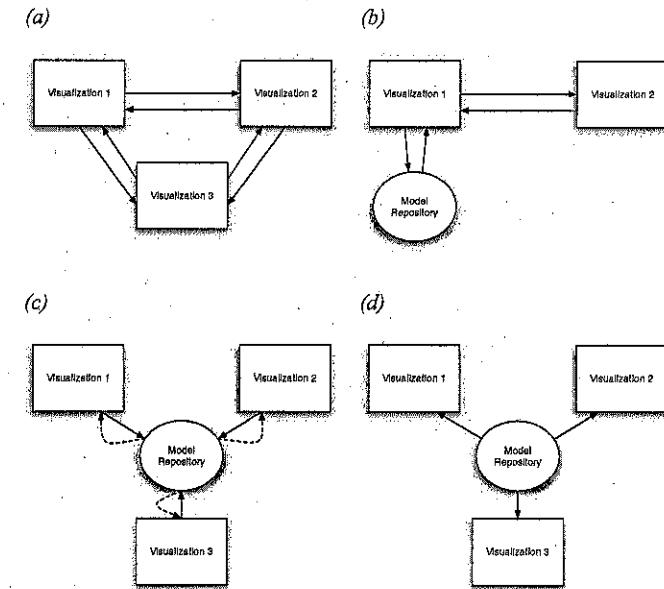
It is important to distinguish the *coordination of multiple visualizations* from *maintaining architectural consistency*. Here, we are only dealing with ensuring that multiple visualizations of the same (parts of the) architectural model are up-to-date with respect to the model. Inconsistencies and conflicts between design decisions stored in the model are a separate issue.

Stakeholders must decide how (and how much) to allow multiple visualizations to display the same architectural information at the same time. If users are only allowed to view information through one visualization at a time, visualizations can be synchronized with the architectural model when they are called up. They can also assume that the model will not change due to some external influence—any changes to the model will be made through this single visualization.

However, if the same information *can* be visualized in many ways simultaneously, it is generally a good idea to synchronize the visualizations in real-time so that they accurately depict the underlying model. This situation is much more complicated, since any visualization

can change the model, and the other visualizations must respond appropriately to that change. If the visualizations include both depiction *and* interaction, then both the depiction and the interaction state of the visualizations must be updated. This might mean changing editing modes, updating menu options, and so on.

Coordinating multiple visualizations can be accomplished through many well-known methods, depending on the situation. For situations where information may be visualized through only one visualization at a time, a simple import-export like method usually works best: initial depictions are created when the visualization is called up and stored (if necessary) when the visualization is dismissed.



**Figure 7-6.** Multiple strategies for coordinating visualizations of the same information: (a) peer-to-peer, (b) master-slave, (c) pull, and (d) push.

Situations where multiple simultaneous visualizations are allowed are harder to deal with. In these cases, four general synchronization strategies are available (see Figure 7-6):

- **Peer-to-peer:** The visualizations maintain their own information about the model, know about each other and explicitly notify one another about changes. These strategies can be brittle because they tend to

tightly couple visualizations. This requires many point-to-point dependencies. The number of dependencies is  $v^2$ , where  $v$  is the number of visualizations. Because of this, the peer-to-peer strategy is most suitable for a small, fixed number of visualizations chosen in advance.

- **Master-slave:** One visualization is primarily responsible for interacting with the model repository, and it serves as the “master” visualization. Other visualizations coordinate through this master, either through a push or pull-based strategy (see below). This works well when one visualization is auxiliary to another; for example, imagine a graphical editor where the main window shows a zoomed-in version of a portion of the architecture, but the corner of the window is portioned off to show a thumbnail of the entire architecture at the same time (for providing context to the user or serving as a navigation aid).
- **Pull-based:** Each visualization repeatedly queries a shared model for changes and updates itself accordingly. This may happen manually—at the user’s request, automatically at periodic intervals, or in response to certain actions (for example, when the user clicks on a new visualization or attempts to make a change to a different visualization). One disadvantage of pull-based strategies is that they may display out-of-date information until they perform a pull operation. Pull-based strategies can be used when the model repository is entirely passive (e.g., a data structure that does not send out events when it changes, or a database system without triggers). When visualization updates are computationally expensive, pull-based strategies can be used to limit how often visualizations are updated. Also, if only one visualization is actually visible at a time, it might not be worthwhile to update a visualization until the user calls it up.
- **Push-based:** Visualizations are notified (and update themselves) whenever the model changes for any reason, usually through an asynchronous event. This is the strategy employed by the model-view-controller pattern. Push-based strategies keep all visualizations up-to-date because any changes are broadcast to each visualization when they occur. These strategies work well when multiple visualizations are presented to the user simultaneously.

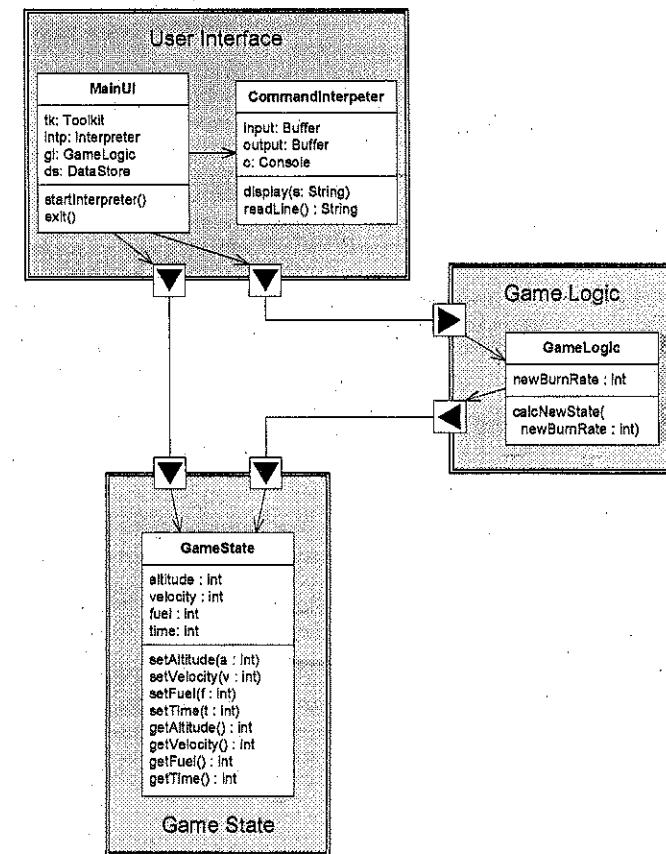


Figure 7-7.  
Visualization  
combining elements  
from xADL and UML.

In situations where the architecture is organized into multiple (partial) models, it is sometimes possible to coordinate access to these models through a single visualization, thus masking some of the differences between notations, or combining the strength of multiple visualizations. Figure 7-7 shows an architecture whose component-and-connector structure is expressed in xADL 2.0, but the detailed design of each component is expressed in UML.

## 7.2.4 Beyond Design: Using Visualization Dynamically

As discussed above, architecture visualizations are primarily used to depict and allow interaction with the design decision that comprise an architecture. However, more advanced and dynamic visualizations can be used to gain an even deeper understanding of the architecture.

We now introduce the concept of ‘effect visualizations.’

**Definition.** An *effect visualization* is a visualization that does not address architectural design decisions directly, but instead addresses the *effects* of architectural design decisions.

For example, imagine an architectural model that contains enough information that it can be used as the basis for a behavioral simulation. The output or results of this simulation are not strictly an architectural model, since they are the results of the design decisions made in the architecture rather than the decisions themselves. Thus, visualizations of such results are not strictly architectural visualizations. These results, however, can be extremely effective in helping stakeholders to better comprehend, implement, or debug the architecture. Therefore, it is useful to consider these effect visualizations in tandem with more traditional architecture visualizations.

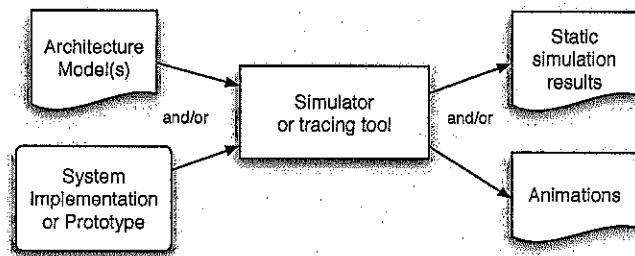


Figure 7-8. Generating effect visualizations.

Figure 7-8 shows common strategies for generating effect visualizations. In general, a rich architectural model serves as one input, and an implemented version of the system or a prototype may serve as another. These are fed into a tool that can analyze or simulate the behavior of the system, or perhaps record and trace the operation of the system implementation or prototype. The output of this tool may include static simulation results or animations that demonstrate the operation of the (simulated) system.

Several architecture tools provide effect visualizations, including Rapide, LTSA, and MTAT. These tools are discussed in more detail later in this chapter, in Section 7.5.

## 7.3 Common Issues in Visualization

While this chapter has focused mainly on techniques for constructing a broad variety of effective visualizations, we can also learn from common mistakes people make in designing visualizations. This section presents some of the more common mistakes people make when developing new visualizations.

### 7.3.1 Same Symbol, Different Meaning

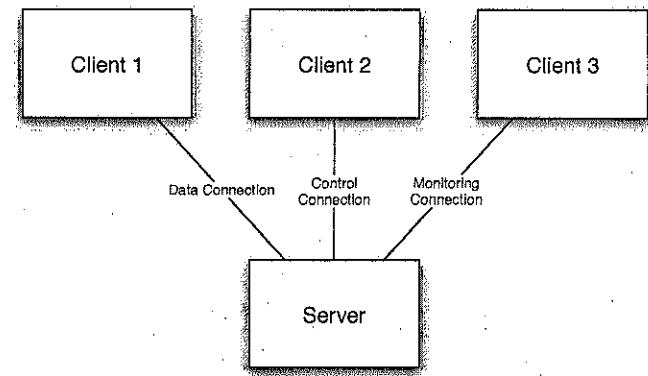


Figure 7-9. Example of “same symbol, different meaning”

When the same symbol is used multiple times in the same visualization, or even across related visualizations, it becomes confusing for users when different meanings are applied to it. This is extremely common for generic symbols such as basic shapes (rectangles, ovals, arrows with default heads). Graphical visualizations provide users with a wide variety of ways of creating distinctive symbols—shapes, decorations, icons, borders, arrowheads, fills, and so on. All of these can be used to make visualizations richer and more precise.

Figure 7-9 shows a simple but deceptive diagram of a client-server system. Here, both the clients and the server are represented by the same symbol (a rectangle), even though they are distinct. The clients and server are all connected with the same type of plain line, although labels indicate that these are clearly different kinds of connections. Additionally, given the

duties of the clients indicated by these connections (data, control, monitoring), it is possible that the clients are not even like one another, even though they appear to be.

### 7.3.2 Differences without Meaning

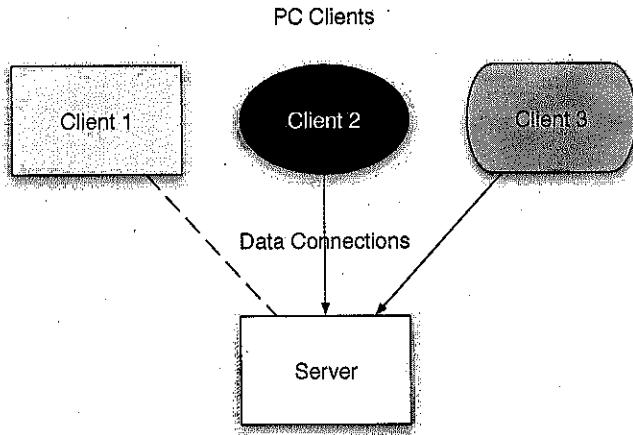


Figure 7-10. Example of “differences without meaning.”

Graphical visualizations in which similar elements are repeated over and over (e.g., the same kinds of components or the same kinds of links) can often appear uninteresting or aesthetically flat. It is common to try to ‘spice up’ such diagrams by adding decorations and other changes to symbols primarily for their aesthetic value—for example, a diagram consisting of many similar components represented as rectangles might assign a different color to each one to avoid the diagram looking monochromatic. This is confusing for users, as it implies a distinction between elements where there is none.

Figure 7-10 shows an example of this situation. Here, the otherwise uniform PC clients are each depicted with a different symbol. Different connection styles (including a random assortment of line styles and arrowheads) connect these uniform clients to the server, all for the same purpose. While this diagram does indeed look more interesting than the one in Figure 7-9, it only serves to confuse. It implies that there is heterogeneity among the clients, and that the connections between the clients and the server are substantially different.

### 7.3.3 Decorations without Meaning

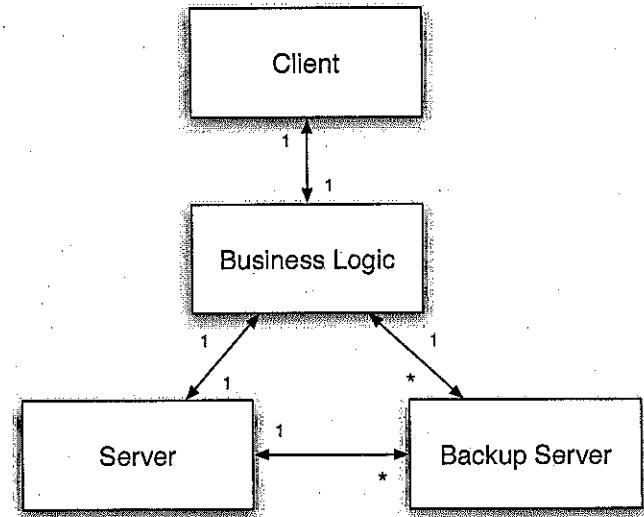


Figure 7-11. Example of “decorations without meaning.”

Some graphical visualizations suffer from a related problem: the consistent inclusion of visual decorations that indicate meaning but are not intended to convey it. A classic example of this is the use of double-headed arrows to indicate a simple connection between two symbols. The arrowheads imply directionality: that information or control is flowing in both directions across the connection. Often, the intended meaning is simply an association: in this case, the arrowheads only serve to confuse the issue by indicating flows where there are none.

Figure 7-11 shows a seemingly innocuous entity-relationship (ER) diagram. These diagrams are used to indicate various elements of a system and their quantity relationships to each other. For example, there is one business logic element in the system, associated with one ordinary server and many backup servers. However, the connections on the diagram are all two-headed arrows. Traditionally, ER diagrams do not include directional associations, since they are not meant to imply dependency, data flow, or any other meaning commonly associated with arrows. These additional decorations may imply things about the relationships between these elements that are simply not true.

### 7.3.4 Borrowed Symbol, Different Meaning

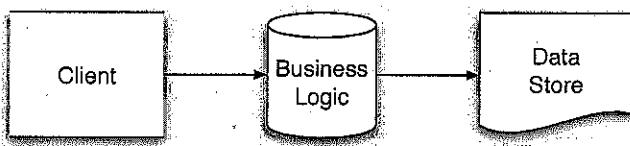


Figure 7-12. Example of “borrowed symbol, different meaning.”

Visualizations are never truly interpreted anew; they are always seen through the lens of the user’s previous experience and knowledge. Experienced users are going to be familiar with a catalog of other visualizations and the symbols and meanings associated with those visualizations. Using symbols that are strongly associated with a different visualization is a good idea if the (rough) meaning of the symbol is brought along as well. Using the same symbol to mean something completely different is a recipe for disaster. For example, using the closed white-headed arrow in a diagram to mean “calls” will likely confuse UML users who will interpret that arrow as meaning “generalization.”

Figure 7-12 shows a simple logical layout for an application. In terms of the issues above, it fares well: three different kinds of symbols are used for three different kinds of components, only one kind of arrow is used and it indicates a calling dependency, and so on. The problem with this diagram lies in the choice of symbols. All these symbols are used in classic flowchart diagrams. The vertical cylinder, used in this diagram to represent the business logic component, is generally used in flowcharting to indicate a data store or disk. The box with a wavy bottom, used here to represent the data store component, is normally used to represent a document or data file. Users familiar with these interpretations might incorrectly infer that the data store was not a component, but simply a file, and that the business logic also acted as some sort of data store.

## 7.4 Evaluating Visualization Techniques

In the past sections, we have explored a number of dimensions that can be used to characterize different visualization techniques. These dimensions can be straightforwardly turned into a rubric for critically thinking about and evaluating different visualizations.

Scope and Purpose	What kinds of models can the technique visualize? Is it an architectural visualization or an effect visualization?
Basic Type	What is the basic type of the visualization:

	graphical? textual? hybrid?
Depiction	How does the visualization depict the model? What are the basic constituents of the depiction?
Interaction	How can stakeholders interact with the visualization? What kind of interface is used? What are the capabilities of the interface?
Fidelity	How faithful is the visualization to the underlying model?
Consistency	How consistent is the use of symbols in depicting information, especially across viewpoints? How consistent are the interaction mechanisms?
Comprehensibility	How easy is it to comprehend the information being visualized? What kinds of information is the visualization optimized for conveying? How well does the visualization leverage existing stakeholder understandings to increase comprehensibility?
Dynamism	How does the visualization use dynamic elements such as animation to depict changes over time?
View Coordination	To what extent is the visualization of multiple views allowed? What strategies are used to coordinate the visualization of multiple views? How effective are these strategies?
Aesthetics	How aesthetically pleasing is the visualization to its users?
Extensibility	How easy is it to tailor or adapt the visualization for new purposes?

This rubric will be applied to several techniques in the remainder of this chapter.

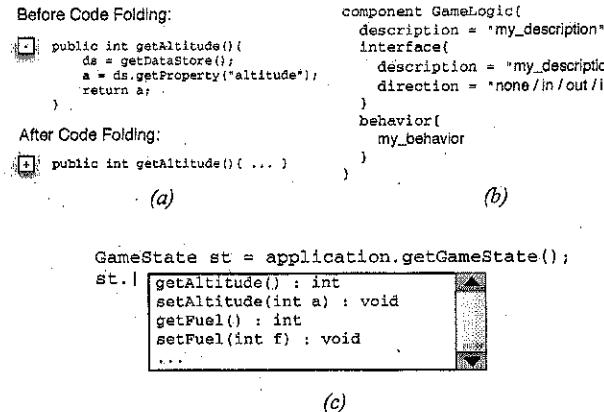
## 7.5 Techniques

This section will survey representative examples of a variety of architecture visualizations that are used in research and practice, from traditional textual and graphical visualizations to more exotic tools that use animation and effect visualizations. Each visualization is evaluated in terms of the above rubric.

### 7.5.1 Textual Visualizations

There are literally as many textual visualizations as there are text editors. Many models’ canonical visualizations are text-based. The most rudimentary text-based visualizations are provided by editors such as Windows Notepad, or ‘pico’ and ‘joe’ on UNIX systems. These editors

display architectural models in a structured text format, in a single font and a single color. Interactions in these basic text editors is limited—users can edit through rudimentary commands like inserting and deleting characters, and copying-and-pasting blocks of text.



**Figure 7-13.** Various advanced techniques used in text visualizations: (a) code folding, (b) templates, and (c) autocomplete.

Enhanced text editors, such as those found in many integrated software development environments, support a similar base feature-set, but offer many improvements as well. These improvements are mostly available through the text editor having some internal knowledge of the syntax or semantics of the underlying model. Common depiction enhancements include syntax coloring and code folding. Editors with syntax coloring support identify segments of text as tokens and color them to represent the type of token (keyword, character string, number, variable, and so on). Code folding is a technique whereby the editor can identify blocks of text and ‘fold’ those blocks into a single line to reduce the amount of detail shown. Both these techniques require that the editor have an understanding of the syntax of the underlying notation. Common interaction enhancements include code completion and templates. Interfaces with code completion allow the user to type some or all of a token, and have the editor present options for completing the token to save typing. Templates allow the user to insert a ‘fill in the blanks’ block of text and then enter data to fill in the missing parameters. Some of these depiction and interaction techniques are shown in Figure 7-13.

#### Evaluation Rubric for Textual Visualizations

Scope and	Depicting and editing models that can be expressed
-----------	--

Purpose	as (structured) text
Basic Type	Textual
Depiction	Lines of text composed of characters; depending on the syntax characters will be grouped into ordered tokens.
Interaction	For basic text editors, insert/delete/copy/paste. Enhanced editors may provide syntax/semantic-aware features like syntax coloring, code folding, code completion and templates.
Fidelity	In general, textual visualizations depict the entire model including all detail.
Consistency	Depends on how well the language syntax is defined; a language with a poorly-designed syntax might use the same token for different purposes in different contexts. Interaction mechanisms are generally consistent because they do not vary.
Comprehensibility	In general, textual visualizations are best for visualizing information that can be organized linearly or hierarchically. They have low comprehensibility for complex models with many interrelated elements, or elements organized in graph structures.
Dynamism	Depends on the editor in use; there are some integrated environments where model changes will cause immediate updates to textual visualizations.
View Coordination	In some integrated environments, textual visualizations can be coordinated with other visualizations of other views via a shared model.
Aesthetics	Depends on the syntax of the language, as well as how the visualization organizes and presents the text. Long, continuous blocks of text tend to be perceived as aesthetically poor; well-organized, attractively colored text tends to be perceived as aesthetically pleasing.
Extensibility	Depends on the editor; some editors provide well-defined extension points for adding in new language syntax and supporting features like syntax coloring and auto-completion for new languages.

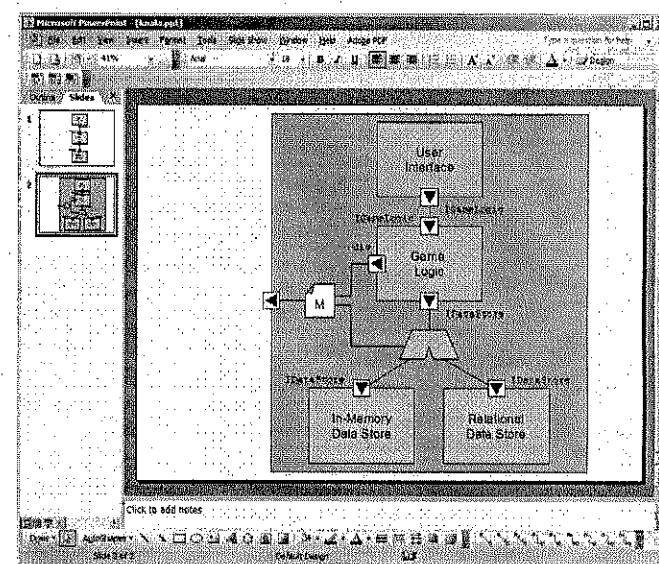
#### 7.5.2 PowerPoint-like

As we have discussed, PowerPoint (and similar graphical editors) [192] [193] [281] are commonly used to capture architectural design decisions

despite the fact that these tools have no support for architectural semantics—they are simply diagram editors. With no real graphical syntax or semantics, the power and allure of PowerPoint-style modeling is not derived from the model or the notation, but from its visualization. From a depiction standpoint, PowerPoint diagrams are generally straightforward and aesthetically pleasing graphics. Text, symbols, and bitmap graphics coexist in depictions as needed. Nothing is hidden: everything in the depiction is visible on the slide at once. Likewise, the slide provides a natural limitation on how much detail can be presented at a time: by having finite boundaries, the canvas of the slide limits the complexity of the visualized information. By building up a slide deck or using PowerPoint's animation capabilities, it is even possible to depict the evolution of an architecture over time.

The most attractive aspect of the PowerPoint visualization, however, is its user interface—how the user creates and manipulates models.

PowerPoint's point-and-click interface allows users to create and manipulate graphical models with great ease and flexibility. Symbols can be created and moved simply by dragging and dropping. PowerPoint 'connector' lines will even maintain their connections as the shapes they connect are moved around the canvas. Users can easily add media from outside sources as well: bitmap graphics, vector graphics, screenshots, and even video and audio clips in nearly any format can be added to the PowerPoint model with only a few mouse clicks.



**Figure 7-14.**  
Screenshot of  
PowerPoint being used  
to draw a Koala-style  
architecture.

Figure 7-14 shows PowerPoint being used to edit a Koala-style architecture. Although the visualization is attractive, certain problems are already apparent. The various elements shown are just independent shapes and text. For example, the interfaces on the components are simply white boxes with black triangles on top; PowerPoint has no concept of an architectural interface. They are not even 'attached' to the rectangles representing components; they simply overlap the edges. Because the diagram is not bound to any semantic representation, keeping it consistent with other models must be done manually. The graphical shapes and decorations available are limited and cannot be easily extended. There are no facilities in the user interface for establishing repeated patterns or for extending the interface to take into account architectural concepts.

#### Evaluation Rubric for PowerPoint-like Visualizations

<b>Scope and Purpose</b>	Visualization of arbitrary collections of symbols, text elements, clip art, and so on.
<b>Basic Type</b>	Hybrid: primarily graphical with some textual annotations and elements.
<b>Depiction</b>	As a canvas containing floating graphical and textual elements, positioned arbitrarily by the user.

	Elements occupying the same space are drawn one on top of the other, with the top-to-bottom ordering determined by the user.
<b>Interaction</b>	Primarily a point-and-click user interface, with options for dragging, dropping, and manipulating elements with the mouse and keyboard.
<b>Fidelity</b>	In general, the underlying model is coupled directly to the visualization and nothing is hidden so the visualization is completely faithful.
<b>Consistency</b>	The user is entirely responsible for developing consistent representations; lack of consistency is a persistent problem in PowerPoint and similar tools.
<b>Comprehensibility</b>	The user is entirely responsible for the comprehensibility of the presented information.
<b>Dynamism</b>	Limited animation facilities are provided for depicting changes over time
<b>View Coordination</b>	In general, it is extremely difficult to coordinate a PowerPoint visualization of information with other visualizations, or even connect elements on multiple slides in the same slide deck to one another.
<b>Aesthetics</b>	Aesthetics are the responsibility of the user; the wide palette of available symbols and decorations gives users enormous freedom to create aesthetically pleasing (or poor) visualizations.
<b>Extensibility</b>	In general, adding new symbols is straightforward; however, extending the user interface to provide new interaction options is more complicated. Scripting capabilities or published APIs that allow extension of the interaction UI may also be available.

### 7.5.3 UML: The Unified Modeling Language

UML as a notation was discussed in Chapter 6. UML has an associated canonical depiction that is primarily graphical. We have seen several examples of UML diagrams already, e.g., in Figure 7-4. Compared to the free-form nature of PowerPoint-like editors that deal in boxes and arrows, UML diagrams are visualizations of more semantically-laden elements such as classes and statechart nodes.

UML concepts are mapped to particular graphical symbols: for example, the ‘generalizes’ relationship between elements is mapped to an arrow with a closed, white, triangular head. While certain concepts (and, as such, their associated symbols) are only present in certain diagrams, diagrams

that incorporate common concepts use the same symbol in each diagram. For example, the ‘generalizes’ relationship is present in both the class and object diagrams, and the same symbol (the closed white arrow) is used to represent the concept in both diagrams. Interestingly, although UML’s syntax is defined in a graphical metamodel, the UML metamodel does not actually map UML concepts to symbols; this mapping is described in other documentation.

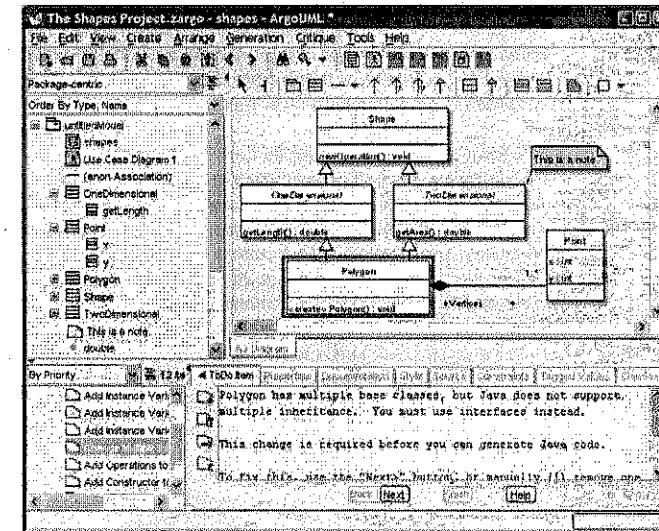


Figure 7-15. Screenshot of ArgoUML.

@@This is taken from the ArgoUML site

Even when taking into account this additional documentation, UML is only associated with a canonical depiction and not a canonical interface. That is, UML’s designers prescribe how UML diagrams should look, but not how the user should interact with them in tools or editing environments. These decisions are left up to individual tool vendors, and tools such as Rational Rose [237] and ArgoUML [2] have different mechanisms for manipulating and otherwise interacting with UML diagrams. Figure 7-15 shows a screenshot from ArgoUML editing a UML model. Note that the canonical graphical visualization is only one part of the environment. Another visualization of the model as a tree is present on the left hand side. Tools accessible from the menu and from the tabbed area below allow the model to be manipulated in different ways.

Tools like Rose and ArgoUML provide compelling user interfaces, but can often blur the distinction between what is provided by the tool and

what is provided by a modeling notation. For example, the screenshot above includes an editor for a “to-do” list. UML itself has no concept of a “to-do” list; this is a feature added by ArgoUML. Users must be cognizant of these distinctions, as they can make it more difficult to integrate multiple tools operating on the same model, or to switch from one environment to another.

```

<UML:Class xmi.id = '723'
    name = 'Data Store'
    visibility = 'public'
    isSpecification = 'false'
    isRoot = 'false'
    isLeaf = 'false'
    isAbstract = 'false'
    isActive = 'false'>

<UML:Association xmi.id = '725'
    name = ''
    isSpecification = 'false'
    isRoot = 'false'
    isLeaf = 'false'
    isAbstract = 'false'>
<UML:Association.connection>
    <UML:AssociationEnd xmi.id = '726'
        visibility = 'public'
        isSpecification = 'false'
        isNavigable = 'true'
        ordering = 'unordered'
        aggregation = 'none'
        targetScope = 'instance'
        changeability = 'changeable'>
    <UML:AssociationEnd.multiplicity>
        <UML:Multiplicity xmi.id = '727'>
            <UML:Multiplicity.range>
                <UML:MultiplicityRange xmi.id = '728'
                    lower = '1'
                    upper = '1'>
            </UML:Multiplicity.range>
        </UML:Multiplicity>
    </UML:AssociationEnd.multiplicity>
    <UML:AssociationEnd.participant>
        <UML:Class xmi.idref = '71F'>
    </UML:AssociationEnd.participant>
</UML:AssociationEnd>

<UML:AssociationEnd xmi.id = '729'
    visibility = 'public'
    isSpecification = 'false'
    isNavigable = 'true'
    ordering = 'unordered'
    aggregation = 'none'
    targetScope = 'instance'
    changeability = 'changeable'>
```

Figure 7-16. Excerpt of an XMI document showing the representation of a UML class and association.

```

<UML:AssociationEnd.multiplicity>
    <UML:Multiplicity xmi.id = '72A'>
        <UML:Multiplicity.range>
            <UML:MultiplicityRange xmi.id = '72B'
                lower = '1'
                upper = '1'>
        </UML:Multiplicity.range>
    </UML:Multiplicity>
</UML:AssociationEnd.multiplicity>
<UML:AssociationEnd.participant>
    <UML:Class xmi.idref = '721'>
</UML:AssociationEnd.participant>
</UML:AssociationEnd>
</UML:Association.connection>
</UML:Association>
```

The canonical graphical visualization is not the only visualization available to UML users. Although it is not part of the core UML standard, it is possible to visualize UML data using text through the use of XMI [210]. XMI is an XML-based format devised to facilitate interchange of models between tools. It is an interchange format in which a UML model (and in fact any model whose syntax is defined in a MOF-based metamodel) can be encoded in XML. XMI helps to draw out the distinction between UML and its canonical graphical visualization. Plain XMI encodes only the information in a UML model, but not information about diagram layout from graphical visualizations. An extension to XMI that includes this information is provided in a separate standard. Figure 7-16 shows an excerpt of an XMI document generated by ArgoUML. Note the amount of text used to depict a simple point-to-point association, as well as the lack of information about graphical depiction, layout, or positioning.

One of the main advantages of UML’s canonical graphical visualization is the (mostly) consistent use of symbols across diagrams and projects. The rationale behind this decision is that it increases the ability of stakeholders who are familiar with UML to quickly understand the meaning of diagrams in different contexts. In this regard, UML’s popularity creates a network effect: the more people that use UML, the more valuable the consistent use of these symbols becomes.

UML’s consistent use of symbols has limitations and disadvantages, however. Symbolic consistency in visualization cannot create semantic precision at the notational level. That is, if the concept of ‘generalization’ is semantically ambiguous, the consistent use of the same arrow shape to depict the concept cannot repair this ambiguity. Additionally, the use of the same set of symbols across project and domain boundaries limits how much UML can be specialized for a particular domain. UML tools and standards do not generally support a lot of customization in UML.

visualizations for individual projects or domains. For example, Rational Rose allows users to associate stereotypes with graphical icons, but will not fundamentally change the symbol of the element to which the stereotype is being applied.

#### Evaluation Rubric for UML Visualizations

<b>Scope and Purpose</b>	Canonical visualization of UML models via (currently) 13 diagram types.
<b>Basic Type</b>	Hybrid: primarily graphical with some textual annotations and elements (e.g., OCL constraints)
<b>Depiction</b>	Each UML diagram type has a canonical depiction. Each diagram type is composed of a handful of basic elements—the class diagram, for example, includes distinctive elements for classes, methods, different kinds of associations, and so on.
<b>Interaction</b>	Depends on the tool in use; different UML tools have different interaction interfaces. Most allow point-and-click editing in the style of PowerPoint, and available editing options are generally guided by UML's syntax and semantics.
<b>Fidelity</b>	As a canonical visualization, these depictions are generally completely faithful.
<b>Consistency</b>	UML attempts to use consistent symbols, even across diagram types; there are small exceptions (an open-headed dashed arrow might indicate a dependency in a class diagram, or a message in a sequence diagram).
<b>Comprehensibility</b>	Most diagrams can be interpreted at a very general level with no prior knowledge. However, properly interpreting each diagram requires specific knowledge of the meaning of each of UML's symbols. Most diagrams have roots in earlier notations (e.g., OMT, and statecharts) that may be familiar to stakeholders outside the context of UML.
<b>Dynamism</b>	Few UML tools use animation to depict changes in the underlying model.
<b>View Coordination</b>	Multiple UML diagrams can be used to represent multiple views of a system; however, there is no agreed-upon standard for linking common information in multiple views. Some editors allow multiple instances of the same element to be present in multiple diagrams simultaneously and will make

	changes to this element simultaneously in all diagrams.
<b>Aesthetics</b>	UML diagrams use a limited set of relatively basic shapes to reduce complexity, although this can make diagrams seem overly simplistic and uniform. Some editors enhance this by allowing UML elements to be colored or enhanced with decorative icons to more clearly indicate element properties, for example.
<b>Extensibility</b>	Depends on the tool/editor in use; most support UML's basic extension mechanisms: stereotypes, tagged values, and constraints. Adding a new diagram type or extending UML's syntax would require major work, however.

#### 7.5.4 Rapide

Earlier in the chapter, we introduced the concept of *effect* visualizations—visualizations that depict the effects of architectural decisions, rather than the decisions themselves. A classic example of this comes from the Rapide project [171], which was introduced in Chapter 6. We have shown several architectural models in Rapide in its canonical textual visualization. However, the real power of Rapide comes from tools that allow users to run simulations of these architectural models. The Rapide simulator takes architecture models in the Rapide notation as input, and then simulates the interaction of the various components as defined by the behaviors specified in the model. Simulation runs generate a stream of events, some of which are causally related to one another. Because Rapide components run in parallel, the results of simulations are not strictly deterministic; repeated simulations of the same architecture can generate different event streams depending on how the simulator's scheduler gives time to the various components.

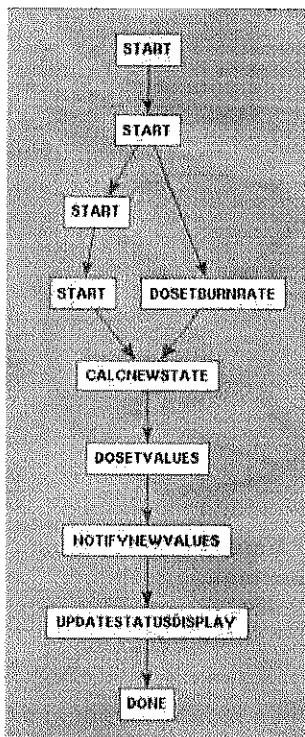


Figure 7-17. Rapide ‘effect visualization’ of the Lunar Lander application.

The result of a Rapide simulation is a directed graph of nodes, with each node representing an event and each edge representing a causal relationship between events. An example, originally presented in Chapter 6, is shown again in Figure 7-17. This can be seen as a kind of visualization of the system and its architecture. Even though it does not necessarily depict specific design decisions, it depicts the direct result of architectural design decisions and can equally serve to provide stakeholders with insights about the workings of the architecture.

#### Evaluation Rubric for Rapide

<b>Scope and Purpose</b>	Specification of architectural structure and component behavior in a textual format; display of simulation results in a graphical format.
--------------------------	---

<b>Basic Type</b>	Architectural models are specified in a textual visualization; effect depictions are graphical.
<b>Depiction</b>	Models in rigorous text format; effect visualizations are directed graphs containing nodes representing events and edges representing causal dependencies.
<b>Interaction</b>	Models are edited in an ordinary text editor; effect visualizations are not editable.
<b>Fidelity</b>	Textual visualization of the model is canonical; effect visualizations show one possible simulation run. Multiple simulations may produce different results in a nondeterministic system.
<b>Consistency</b>	Limited vocabulary of symbols ensures consistency.
<b>Comprehensibility</b>	Architectural models can be difficult to write and understand, although this is largely due to the complexity of the underlying notation. Effect visualizations are straightforward to understand, although complex systems may generate very large intertwined graphs that are difficult to interpret.
<b>Dynamism</b>	No support.
<b>View Coordination</b>	Effect visualizations are generated automatically from architectural models.
<b>Aesthetics</b>	Models are in a familiar programming-language style although the vocabulary of operators is fairly large. Effect visualization graphs are simple and unadorned.
<b>Extensibility</b>	Difficult to extend; Rapide and its toolset is a relative “black box.”

#### 7.5.5 The Labeled Transition State Analyzer (LTSA)

The Labeled Transition State Analyzer (LTSA) project from Imperial College in London, UK is a way of analyzing and simultaneously visualizing concurrent systems [177]. A system in LTSA is modeled as a set of interacting finite state machines. Users specify component behaviors in a compact process algebra called FSP; FSP is then compiled into state machines with labeled transitions. The LTSA tools can visualize these state machines graphically using a traditional nodes-and-arrows visualization.

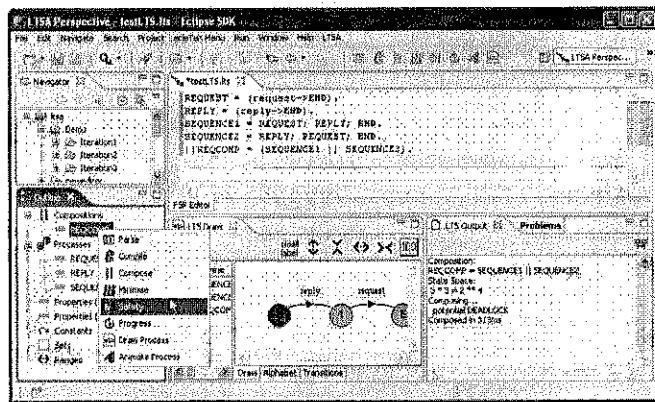


Figure 7-18. Screenshot of the LTSA tool.  
@@from the LTSA site

Figure 7-18 shows a screenshot of the LTSA tool. Multiple concurrently-maintained visualizations are shown. The upper-right area shows the canonical textual visualization of the model: raw FSP. To its left is a tree-based visualization of the project's organization. The lower-center section shows a graphical visualization of the FSP model as a state-transition diagram. The lower-right shows a textual effect visualization that results from automated analysis of the FSP model; animated effect visualizations are also available.

A unique strength of LTSA is its ability to employ dynamic visualizations. Because LTSA deals with concurrency, its visualizations have a specific need to capture and display the state of described systems over time. LTSA employs two strategies for this purpose, both employing animation. First, when an LTS is simulated and its state machines are being viewed, the current state and state transitions are animated atop the nodes-and-arrows visualization shown above. Second, and more interestingly, LTSes can be hooked up to animated visualizations that use animation to directly show what is going on in the system from a domain-specific perspective.

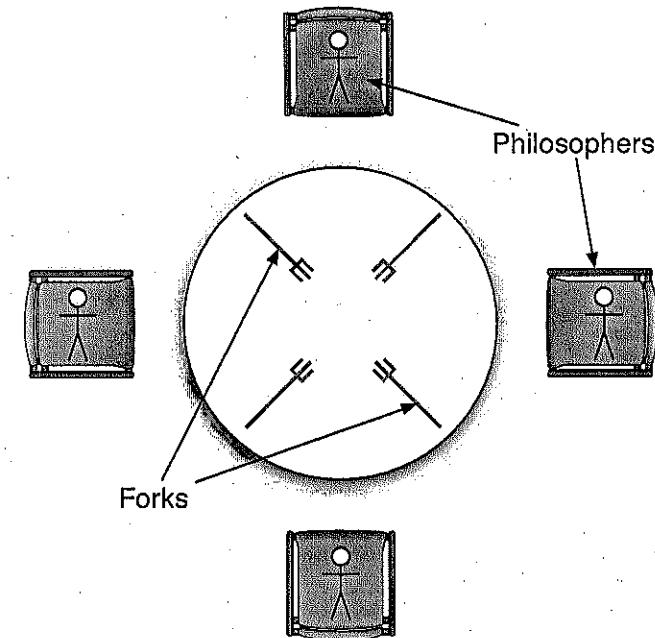


Figure 7-19. Four dining philosophers.

One of the examples included in the LTSA documentation is an implementation of the famous 'dining philosophers' problem shown in Figure 7-19, a classic problem in dealing with concurrency. In this problem, a set of philosophers sit around a circular table. In between each pair of philosophers is a fork. Philosophers need to pick up both their adjacent forks to eat, but are also constrained by a set of rules as to when they can pick up and put down forks. The challenge in the problem is coming up with a set of rules such that all philosophers get to eat periodically and the system does not enter a locked state (for example, in which each philosopher picks up one fork and none will put theirs down).

The LTSA tools model the philosophers as communicating state machines, but can also visualize the models as a diagram of a table surrounded by philosophers, similar to what is shown in Figure 7-19. State changes, like a philosopher acquiring a chopstick, are visualized as an actual picture of a philosopher picking up a chopstick. Simulations of other applications, such as air traffic control, use similar domain-specific visualizations hooked up directly to the component behavior simulators (such as pictures

of airplanes circling and landing). Unlike Rapide, which only lets you visualize event traffic in a graph after-the-fact, LTSA allows users to visualize the system being simulated in real time, using animations and symbols that are directly drawn from the real domain. Although users of LTSA have to spend time and effort to construct these domain-specific visualizations for each application, their value comes from the fact that they go a long way to communicate the real meaning of abstract state machines. Whereas it may be difficult to understand the meaning of a particular state transition in a nodes-and-arrows diagram, it is much easier to understand a picture of a philosopher actually picking up a chopstick.

#### Evaluation Rubric for LTSA

<b>Scope and Purpose</b>	Coordinated visualization of FSP models and different effect visualizations.
<b>Basic Type</b>	Multiple textual and graphical model views and effect visualizations.
<b>Depiction</b>	FSP models are visualized both in text and in graphical state-transition diagrams. Effect visualizations may be textual, animated on the state-transition diagrams, or custom and domain-specific.
<b>Interaction</b>	An integrated set of tools allow the user to manipulate FSP models in both text and graphical visualizations.
<b>Fidelity</b>	Coordination between visualizations and models are maintained automatically; graphical visualizations may elide some information.
<b>Consistency</b>	Limited vocabulary of symbols and concepts helps to ensure consistency.
<b>Comprehensibility</b>	FSP is a complex textual notation but is somewhat easier to understand than other formalisms. State-transition diagrams are straightforward and their format is well-known. Custom domain-specific visualizations can increase comprehension substantially by tying models back to domain concepts graphically.
<b>Dynamism</b>	Animation on state-transition diagrams and custom domain-specific visualizations.
<b>View Coordination</b>	Views are coordinated automatically.
<b>Aesthetics</b>	Well-known state-transition diagrams are easy to interpret; domain-specific visualizations tie abstract models to concrete real-world concepts.

<b>Extensibility</b>	New custom domain-specific visualizations can be added as plug-ins.
----------------------	---

#### 7.5.6 xADL 2.0

The syntax of the xADL 2.0 language is defined in a set of XML schemas. As such, the canonical visualization for xADL 2.0 files is textual, in the XML format that conforms to the syntax prescribed by the schemas. One of the most interesting aspects of xADL 2.0, however, is that its canonical visualization is rarely (if ever) used or even seen by its users. Tools that support xADL 2.0 modeling provide a variety of alternative visualizations, both graphical and textual [55]. Some of these visualizations include:

##### xADL<sup>ite</sup>

The xADL<sup>ite</sup> visualization has been used throughout this book to describe various architectures. xADL<sup>ite</sup> is a textual visualization that captures xADL 2.0 models using textual tokens organized in a manner similar to C-like programming languages: hierarchical blocks are surrounded by curly braces, the '=' operator is used to denote assignment, double-quotes surround string values, and so on. This visualization was specifically crafted to capture all the data in a xADL 2.0 model in a compact format, using as few extraneous characters as necessary. The programming-language-like symbology was chosen due to the popularity of this organization: experienced software developers are comfortable with these symbols and organization and can read it easily without additional training. From a user-interface perspective, xADL<sup>ite</sup> files are written and manipulated using standard text editors.

##### ArchEdit

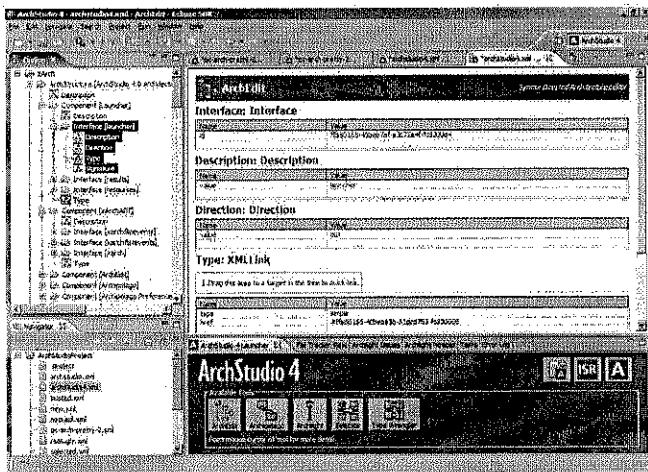


Figure 7-20. ArchEdit screenshot.

ArchEdit, shown in Figure 7-20, is a tool that provides a semi-graphical visualization of xADL 2.0 models. The document structure is depicted in a tree format with selectable nodes. When a node is selected, text attributes of that node are displayed for editing. Although the information in this view is organized hierarchically (much like the XML or xADL Lite visualizations), the user interface of ArchEdit is far more interactive. ArchEdit has a point-and-click interface that not only allows users to expand and collapse subtrees of the document, but also provides context-sensitive menus that provide the user specific options to add, remove, or manipulate elements. ArchEdit provides a *syntax-directed* visualization: the user interface and what is displayed on the screen are both derived, at least partially, from the syntax of xADL 2.0 itself. For example, when you right-click on an element in ArchEdit, it brings up a menu of children that can be added to that element. The list of available children is generated based on the syntax of the xADL 2.0 language, and is not hardcoded in the tool itself. For a language with malleable syntax like xADL 2.0, syntax-directed visualizations and other tools become even more valuable. The primary disadvantage of (even the best) syntax-directed visualizations is that the syntax of the underlying notation drives how the information is visually presented; if the notation is tree-like and hierarchical, it is likely that a syntax-directed visualization of the notation will also employ trees and hierarchy.

#### Archipelago

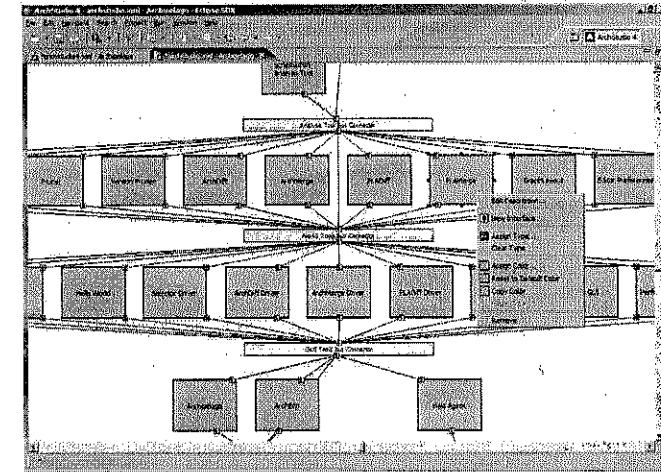


Figure 7-21. Archipelago screenshot.

Archipelago, shown in Figure 7-21, is a tool that provides graphical visualizations of xADL 2.0 models. Archipelago's visualizations are semantically-aware, meaning that specific depictions and behaviors are built into Archipelago to represent and interact with different xADL concepts. For example, components and connectors are represented as rectangles, interfaces are represented as square endpoints attached to the borders of component and connector rectangles, and links are represented as splines. Unlike ArchEdit, which can adapt its user interface automatically to new syntactic elements, Archipelago must be extended to support new xADL 2.0 concepts. However, Archipelago can provide much more intuitive visualizations to its users: it is much easier to understand an architectural topology by looking at a box-and-line graph than a flat list of components, connectors, and links.

Archipelago's internal architecture relies heavily on plug-ins for implementing visual elements and their graphical representations as well as behaviors—how Archipelago reacts to user input and external events. In fact, Archipelago itself is really a small core of extension points; almost all of its behavior is implemented by plugins. This makes Archipelago a highly flexible environment for adding new visual elements and behaviors, a real necessity when the underlying notation being visualized (xADL 2.0) is itself modular and extensible.

The primary disadvantage of fully semantics-aware editors such as Archipelago is the expense of creating and maintaining them. Users expect

intuitive, comprehensive, custom behavior tailored to individual notations, and for more extensive notations this can be quite costly to build. Archipelago attempts to limit this cost by using a modular architecture, but this cannot reduce the complexity of such editors to anywhere near the level of simpler syntax-directed editors.

#### MTAT

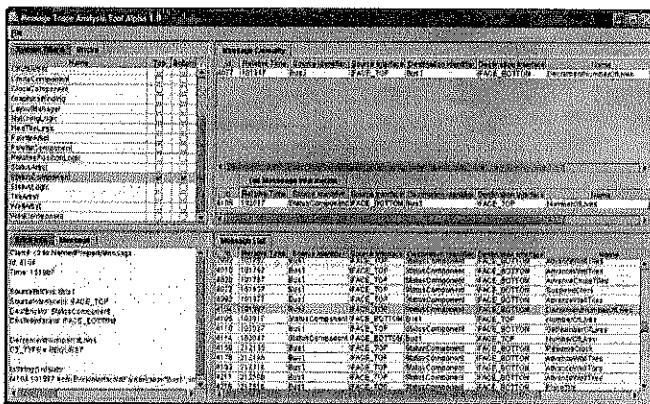


Figure 7-22. MTAT screenshot.

The Message Tracing and Analysis Tool (MTAT) [116], shown in Figure 7-22, provides additional visualization support for xADL 2.0 architectures that are mapped to implementations composed of components that interact using asynchronous events. Like Rapide and LTSA, MTAT's visualizations capture a dynamic aspect of a system's architecture, namely the sending and receiving of events. However, unlike Rapide and LTSA which only work on simulated architectures, MTAT provides a unified visualization of two lifecycle activities: architecture design and implementation. Events visualized in MTAT are real events sent among components in a real system. Animation can overlay these events on structural diagrams of the architecture visualized in Archipelago, and the user can 'follow' a string of events from component to component, watching how the running application works at the same time.

#### Evaluation Rubric for xADL 2.0 Visualizations

<b>Scope and Purpose</b>	Multiple coordinated textual, graphical, and effect visualizations of xADL 2.0 models.
<b>Basic Type</b>	Coordinated textual, graphical, and effect.

<b>Depiction</b>	Textual visualizations as XML or xADL Lite; graphical visualizations as trees and text (in ArchEdit) or symbol graphs (in Archipelago); hybrid effect visualizations in MTAT.
<b>Interaction</b>	Multiple coordinated editors each with their own interaction paradigm that resembles comparable editors for other notations.
<b>Fidelity</b>	Textual visualizations and ArchEdit display entire model without leaving out detail; various graphical visualizations elide some detail.
<b>Consistency</b>	Each visualization uses its own method of depicting concepts, although features such as common icons unify them. Interaction mechanisms are also optimized for the particular visualization, although they tend to be consistent with similar tools for other notations.
<b>Comprehensibility</b>	Different visualizations have different levels of comprehensibility. Graphical visualizations tend to be easier to understand than textual notations, but they leave some information out. Different visualizations are optimized for displaying different kinds of information.
<b>Dynamism</b>	Visualizations such as MTAT use animation to depict the behavior of running systems; other visualizations are coordinated "live" so that changes in one visualization appear immediately in others.
<b>View Coordination</b>	Different visualizations are coordinated through a common model repository that maintains an in-memory representation of the underlying xADL model.
<b>Aesthetics</b>	Different visualizations attempt to increase aesthetic appeal by being specialized for depicting a particular kind of information.
<b>Extensibility</b>	New visualizations can be added by hooking into the common model repository; visualizations such as Archipelago are also extensible through their own internal plug-in mechanisms.

## 7.6 End Matter

In this chapter, we have focused on the role of visualization in software architecture-based development. Visualizations comprise *depiction* (how a set of design decisions is visually presented) and *interaction* (how stakeholders interact with, explore, and manipulate those depictions).

Perhaps the most important lesson from this chapter is that visualizations are not the same things as their underlying modeling notations. Every modeling notation has at least one canonical visualization—it may be textual, graphical, or a combination of both. It is difficult and sometimes counterintuitive to try to mentally separate the information content of a model from its canonical visualization, but making this distinction is useful. Once this distinction is made, it is possible to think about alternative or coordinated visualizations for the same model. It is also possible to separate the strengths and weaknesses of a modeling notation from the strengths and weaknesses of how that notation is visualized. This distinction also helps to explain phenomena like the use of PowerPoint-like tools for architecture modeling. Here, the visualization is extremely mature and versatile, but the underlying model is devoid of semantics. This makes these tools attractive, but dangerous to use in the long run.

When selecting visualizations for a project, do not neglect effect visualizations. Recall that effect visualizations do not visualize architectural design decisions directly, but the results of applying some process to those design decisions—analysis, simulation, and so on. Often, so much focus is put onto model visualization that these effect visualizations get short shrift. Remember that analysis and simulation results are critical and must be interpreted correctly; this can be made substantially easier with the use of appropriate effect visualizations.

Used appropriately, visualizations can make working with, understanding, exchanging, and communicating about architectural design decisions much easier. To maximize this effect, select visualizations with high degrees of fidelity, consistency (both internal and external), comprehensibility, dynamism, and so on. These decisions should be considered in the context of the target stakeholders and their own needs, skills, and prior experiences.

Visualizations can be seen as the “user interfaces” to architectural models. In many ways, they fulfill the same role as a user interface in a software system. They define the look and feel of the underlying model to stakeholders. They can make it easier to work with the underlying concepts and semantics, but do not modify them. Because of this, even the best visualizations cannot rectify semantic problems in their target notations, but they can add substantial value to already-adequate notations, and have a tremendous effect on the practical usability of those notations.

For these reasons, it is important to consider visualizations—not just notations—up front in a software development effort. One key factor to

keep in mind while selecting visualizations is the set of stakeholders that will be using them. Visualizations can take complex models and present them (or a subset of them) in a way that makes intuitive sense to stakeholders. The kinds of visualizations that are most useful for a project manager, for example, are not the same as those that are useful for a software engineer. While canonical visualizations are always available, remember that alternatives are often available as well.

The decision to develop a new visualization should be made with great care. As noted in the chapter, new visualizations can be very costly to develop and maintain. If possible, leverage extensibility mechanisms available in existing visualizations rather than developing one from scratch. Developing a new visualization can be a viable strategy in certain circumstances. Some notations, particularly esoteric or research-based notations, may have valuable semantics or analysis capabilities but lack good visualization support. When developing a family of systems in a particular domain (see Chapter 15), creating new domain-specific visualizations may also be valuable, and the cost is amortized over all projects that use the visualization.

## 7.7 Review Questions

1. What is a visualization? What two key elements comprise a visualization?
2. What is the difference between a visualization and a modeling notation? What is a canonical visualization?
3. Identify and describe the two primary categories of visualizations.
4. What are hybrid visualizations? Identify a hybrid visualization and describe why it is a hybrid.
5. What is the relationship between visualizations, viewpoints, and views?
6. Enumerate and describe some criteria that can be used to evaluate visualizations.
7. When should you consider creating a new visualization? Enumerate and describe some strategies for creating an effective new visualization.
8. What does the work of Edward Tufte have to say about software architecture visualizations? What are his key insights?
9. Enumerate and describe some strategies for coordinating multiple visualizations.
10. What are effect visualizations? Where do they come from? How are they different from ordinary architecture visualizations?
11. Enumerate and describe some common problems that arise in architecture visualization.

12. What kinds of visualizations are associated with UML? How do these complement and differ from each other?
13. How do Rapide and LTSA utilize effect visualizations?
14. What kinds of visualizations are associated with xADL 2.0? What are the strengths and weaknesses of these visualizations?

## 7.8 Exercises

1. Identify a notation that is supported by two different visualizations (e.g., a graphical and textual visualization). Model a system of your choosing, such as Lunar Lander, in both visualizations. Compare and contrast the experiences, and note especially what kinds of information were easy, hard, or impossible to capture in either.
2. Acquire and install a system that uses effect visualizations, such as Rapide, LTSA, or MTAT. Find a partner and have each of you model a small system using these tools. Trade systems and see how the effect visualizations can be used to help understand each others' models.
3. Choose one or more architectural visualizations not described here and evaluate it using the evaluation rubric presented in the chapter. What are their strengths and weaknesses?
4. Choose an architecture modeling notation and construct a simple novel visualization for it. For example, develop a simplified graphical editor that focuses only on a few kinds of elements, or use a translation technology such as XSLT to transform a complex textual depiction into something more readable.
5. Identify an unusual user interface feature (depiction, interaction, or both) that you have seen outside the context of architecture visualizations—perhaps in another application, a Web interface, or a video game. How might you apply this to architecture visualization? Would it be an improvement or a hindrance?
6. Choose an architecture visualization (or set of visualizations) not presented here. Does it follow the guidelines in this chapter for effective visualizations? Does it exhibit any of the common problems associated with visualizations? Develop a constructive critique of the visualization along these lines.

## 7.9 Further Reading

Most of the visualizations you will encounter are canonical visualizations, and so are documented in the same places as their associated tools or underlying notations. Such is the case for PowerPoint-like tools [192] [193] [281] and UML [24], as well as several others. It is also interesting to investigate related visualizations that are not canonical, such as XMI [210]. Systems like Rapide [171] and LTSA [177] are interesting for their use of effect visualizations.

The work of Edward Tufte [292, 293], cited in a sidebar in this chapter, is excellent reading for anyone who wants to present complex information in a clear, coherent way. Although he focuses mainly on the display of scientific, quantitative data, many of his ideas are easily translated to other domains and applications.

## CHAPTER 8

## 8 Analysis

Rigorous models of software architectures, which were discussed in the preceding chapters, present a number of advantages over informal “boxes and lines” diagrams. They force the software architect to address issues he might have otherwise missed or ignored. They allow more precise communication among the system’s various stakeholders. They form a solid blueprint for the system’s construction, deployment, execution, and evolution. And they typically present more detail about the architecture than do informal models, so that more questions can be asked and answered about them more precisely — although there are certainly times where sufficient understanding about certain aspects of a system can be obtained even from informal models.

**Definition.** Architectural analysis is the activity of discovering important system properties using the system’s architectural models.

Getting early, useful answers about relevant aspects of the system’s architecture can help identify inappropriate or incorrect design decisions before they are propagated into the system, thus reducing the risk of system and project failures. It is important for a software architect, as well as other system stakeholders, to know which questions to ask about the architecture and why, how to ask them, and how best to ensure that they can be answered by extrapolating and interpreting the necessary information captured the architecture’s model.

All models will not be equally effective in helping to determine whether a given architecture satisfies a certain requirement. For example, consider the diagram representing the Lunar Lander architecture in Figure 8-1, initially introduced in Chapter 6. This diagram might help the architect get clarifications from the system’s customer and vice versa; it may also be (informally) analyzed by a manager to ensure that the project’s scope is appropriate. At the same time, such an early, informal model will not always be useful for communicating with, and within, the system development teams. The model, for example, does not help answer questions such as how exactly the components (that is, the model’s boxes)

interact, where they are deployed with respect to each other, and what the nature of their interactions (that is, the model’s lines) is.

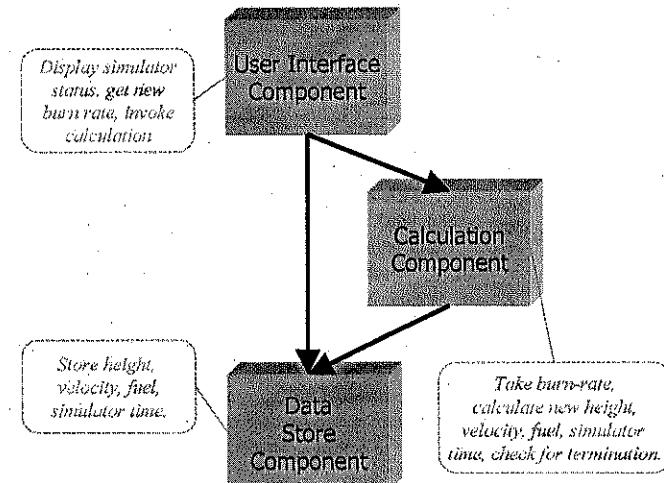


Figure 8-1. A diagram informally representing the Lunar Lander architecture using Microsoft PowerPoint.

On the other hand, a more formal architectural model of the given system may precisely define component interfaces, the conditions under which invoking a given interface is legal, a component’s internal behavior, its legal external interactions, and so on. An example such model of the Lunar Lander architecture was given in Chapter 6; it is shown again in Figure 8-2. This model can be analyzed for a number of properties. For example, the model can help to ensure component composability into the system in the manner specified by the architectural configuration. After that analysis is successfully completed, the individual components may be assigned to developers for implementation. In some cases individual component models may be used instead in further analysis to discover closely matching existing components to be grabbed off-the-shelf and reused in the new system. Yet another alternative would be to analyze the component model by an automated code generation tool whose output would be the component’s partial implementation in a given programming language.

Figure 8-2. A partial, formal model of the Lunar Lander architecture

```

Component DataStore
Port getValues
Port storeValues
Computation

```

corresponding to the diagram from Figure 8-1. The architecture is modeled using the Wright ADL.

```
Component Calculation
  Port getValues
  Port storeValues
  Port calculate
  Computation
```

```
Component UserInterface
  Port getValues
  Port calculate
  Computation
```

```
Connector Call
  Role Caller = call → return → Caller[]§
  Role Callee = call → return → Callee []§
    Caller.call → Callee.call → Glue
  Glue = []Callee.return → Caller.return → Glue
    []§
```

```
Configuration LunarLander
Instances
  DS : DataStore
  C : Calculation
  UI : UserInterface
  CtoUIgetValues, CtoUIstoreValues, UItoC, UItoDS : Call
```

```
Attachments
  C.getValues as CtoUIgetValues.Caller
  DS.getValues as CtoUIgetValues.Callee

  C.storeValues as CtoUIstoreValues.Caller
  DS.storeValues as CtoUIstoreValues.Callee

  UI.calculate as UItoC.Caller
  C.calculate as UItoC.Callee

  UI.getValues as UItoDS.Caller
  DS.getValues as UItoDS.Callee
```

End LunarLander.

At the same time, such a rich model may not be the most effective means for answering questions about the given project's scope or about the resulting system's satisfaction of key requirements. Such questions may be more effectively answered by the system's less technical stakeholders, such as managers and customers, through informal, perhaps manual analysis of less rigorous and detailed models.

It is also crucial to recognize that analyzing a software architecture does not have the same objectives, and is not dealing with the same issues, as analyzing software programs. Architects will have to determine which problems identified in their architectures are critical, and which ones are not. Some problems uncovered by analysis may be acceptable if the system is still undergoing architectural design, e.g., if certain parts of the architecture are still missing.

Another dimension to this issue is induced by off-the-shelf reuse of existing functionality. In naive theory, software developers should strive to achieve "perfect" matches among their system's components: each service provided by a given component will be needed by one or more components in the system, and each service required by a given component will be provided by another component in the system. In other words, there is neither any unneeded functionality provided in the system, nor is there any needed functionality missing from the system. Systems developed in this manner are simpler and conceptually cleaner. However, this does not work in most large software systems, for which architecture-based development is geared. Most such systems involve the reuse of off-the-shelf functionality, and design and implementation of extensible components that will be usable in multiple systems. Therefore, certain mismatches among the components in a given architecture may be not only acceptable, but also desirable in this larger context.

The objective of this chapter is to present and relate different facets of architectural analysis. To this end, this chapter organizes the discussion around seven dimensions of concern relevant to architectural analysis:

1. the goals of analysis,
2. the scope of analysis,
3. the primary architectural concern being analyzed,
4. the level of formality of the associated architectural models,
5. the type of analysis,
6. the level of automation,
7. the system stakeholders to whom the results of analysis may be relevant,
- and, finally,
8. the applicable analysis techniques.

The remainder of the chapter will expound upon each of the seven dimensions, and will discuss how they relate to and sometimes constrain each other.

#### Outline of Chapter 8

8. Analysis
8.1 Analysis Goals
8.1.1 Completeness
8.1.2 Consistency

- 8.1.3 Compatibility
- 8.1.4 Correctness
- 8.2 Scope of Analysis
  - 8.2.1 Component- and Connector-Level Analysis
  - 8.2.2 Subsystem- and System-Level Analysis
  - 8.2.3 Data Exchanged in the System or Subsystem
  - 8.2.4 Architectures at Different Abstraction Levels
  - 8.2.5 Comparison of Two or More Architectures
- 8.3 Architectural Concern Being Analyzed
  - 8.3.1 Structural Characteristics
  - 8.4 Level of Formality of Architectural Models
  - 8.5 Type of Analysis
  - 8.6 Level of Automation
  - 8.7 System Stakeholders
  - 8.8 Analysis Techniques
    - 8.8.1 Inspections and Reviews
    - 8.8.2 Model-Based Analysis
    - 8.8.3 Simulation-Based Analysis
  - 8.9 End Matter: Tying It All Together
  - 8.10 Review Questions
  - 8.11 Exercises
  - 8.12 Further Reading

## 8.1 Analysis Goals

As with analysis of any software artifact, the analysis of architectural models can have varying goals. Those goals may include early estimation of system size, complexity, and cost; adherence of the architectural model to design guidelines and constraints; satisfaction of system requirements, both functional and non-functional (see Chapter 12); assessing correctness of the implemented system with respect to its documented architecture; determining the opportunity for reuse of existing functionality when implementing parts of the modeled system; and so forth. We categorize such architectural analysis goals into four categories, as discussed below. We refer to these as the four *Cs* of architectural analysis.

### 8.1.1 Completeness

Completeness is both an external and an internal analysis goal. It is *external* with respect to system requirements. The main goal of assessing an architecture's completeness in this context is to establish whether it adequately captures all of a system's key functional and non-functional requirements. Analyzing an architectural model for external completeness is non-trivial. Software systems for which an architecture-centric development perspective is most useful are often large, complex, long lived, and dynamic. In such settings, both the captured requirements and

the modeled architecture may be very large and complex, and may be captured using a multitude of notations of various levels of rigor and formality. Furthermore, both will likely be specified incrementally and will change over time, so that the system's engineers will need to carefully select points at which external completeness of the architecture can and should be assessed meaningfully.

Analyzing an architecture for *internal* completeness establishes whether all of the system's elements have been fully captured, both with respect to the modeling notation, and with respect to the system undergoing architectural design.

Establishing the completeness of the model with respect to the modeling notation (recall Chapter 6) ensures that the model includes all the information demanded by the notation's syntactic and semantic rules. For example, the architectural model depicted in Figure 8-2 is captured in the Wright architecture description language and thus must adhere to Wright's syntax and semantics. Given this choice of modeling notation, the component and connector instances in the *Configuration* portion of the model must be attached to one another (see the *Attachment* statement in Figure 8-2) according to the rules of Wright: a component's port must be attached to a connector's role and can never be attached to another component's port.

Note, however, that fulfilling the modeling requirements of a language such as Wright does not ensure that the architecture is in fact captured completely. Wright is agnostic as to whether the architect accidentally omitted a major system component, or whether a specified component's interface is missing critical services. Establishing the completeness of the architectural model with respect to the system being designed requires checking—often manually, as will be further discussed later in the chapter—whether there are missing components and connectors in the architecture; whether the specified components' and connectors' interfaces and protocols of interaction are fully specified; whether all of the dependencies and interaction paths are captured by the system's architectural configuration; and so on.

In principle, internal completeness is easier to assess than external completeness, and is amenable to automation. A number of software architecture analysis techniques have focused on this very analysis category, as will be further elaborated later in this chapter.

### 8.1.2 Consistency

Consistency is an internal property of an architectural model, which is intended to ensure that different elements of that model do not contradict one another. The need for consistency derives from the fact that software

systems, and thus their architectural models, are complex and multi-faceted. As a result, even if no architectural design decisions are invalidated during the architectural design process, capturing the details of those decisions during architecture modeling may result in many inadvertently introduced inconsistencies. Example inconsistencies in a model are

- name inconsistencies,
- interface inconsistencies,
- behavioral inconsistencies,
- interface inconsistencies, and
- refinement inconsistencies

Each is discussed in turn below.

### Name Inconsistency

*Name* inconsistencies can occur at the level of components and connectors, or at the levels of their constituent elements, such as the names of the services exported by a component. The experience from using programming languages may suggest that name inconsistencies are trivial and easy to catch. However, this will not always be the case, especially at the architectural level. First, multiple system elements and/or services may have similar names. For example, a large system may have two or more similarly named GUI rendering components; likewise, a large GUI component may provide two or more similarly named widget rendering services. Determining that the wrong component or service is accessed may be difficult.

The second problem with possible name inconsistencies concerns the richness of design choices available to the software architect. In a programming language such as Java, attempting to access a non-existent class or method will most often result in compile-time errors which the engineer must correct before moving on. This is a by-product of relatively tight coupling of different program elements: early binding, type checking, and synchronous point-to-point procedure call semantics. On the other hand, a software architect may rely on highly decoupled architectures characterized by publish-subscribe or asynchronous event broadcast component interactions. Furthermore, the architecture may be highly adaptable and dynamic, such that tracking all name mismatches at a given time may be meaningless: a component or service referred to in the architecture may be unavailable currently, but will be added to the system by the time it is actually needed.

### Interface Inconsistency

*Interface* inconsistencies encompass the issues present in name inconsistencies. Specifically, all name inconsistencies are also interface

inconsistencies, but not the other way around. A component's required service may have the same name as another component's provided service, but their parameter lists, as well as parameter and return types, may differ.

For illustration, consider the following. The interface of a required service in a simple *QueueClient* component, specified using an architecture description language, may be as follows:

```
ReqInt: getSubQ(Natural first, Natural last, Boolean remove)
         returns FIFOQueue;
```

This interface is intended to access a service that returns the subset of a FIFOQueue between the specified *first* and *last* indices. The original queue may remain intact, or the specified sub-queue may be extracted from it, depending on the value of the *remove* parameter.

On the other hand, the *QueueServer* component providing the service may export two *getSubQ* interfaces as follows:

```
ProvInt1: getSubQ(Index first, Index last)
           returns FIFOQueue;

ProvInt2: getSubQ(Natural first, Natural last, Boolean remove)
           returns Queue;
```

All three interfaces have identical names, so it can be immediately observed that there is no name inconsistency. However, the three interfaces' parameter lists and return types are not identical. Specifically:

1. The types of the *first* and *last* parameters in the required interface *ReqInt* and the provided interface *ProvInt1* are different.
2. The required interface *ReqInt* introduces a Boolean *remove* parameter, which does not exist in *ProvInt1*.
3. Finally, the return types of the provided interface *ProvInt2* and required interface *ReqInt* are different.

Whether these differences result in actual interface inconsistencies will depend on several factors. If the *QueueClient* and *QueueServer* were objects implemented in a programming language such as Java, and their respective provided and required interfaces denoted method invocations, the system might not even compile. However, as has been demonstrated repeatedly throughout this book, software architecture provides a much richer set of choices to an engineer. Consider all three differences

between the provided and required interfaces, and their impact on potential interface inconsistency.

1. If the data type `Natural` is defined to be a subtype of `Index`, then requesting the `getSubQ` service will not cause a type mismatch between `ReqInt` and `ProvInt1`. Instead, a simple type cast will occur and the request will be serviced normally.
2. If the connector between `QueueClient` and `QueueServer` components is a direct procedure call, then an interface inconsistency will occur between `ReqInt` and `ProvInt1` because of the additional parameter in the required interface. No such inconsistencies will occur between between `ReqInt` and `ProvInt2`, which have identical parameter lists. On the other hand, if the two components interact via an implicit invocation mechanism, such as an event connector, the connector may simply package the request such that the `QueueServer` component can still service it via the `ProvInt1` interface, by ignoring the `remove` parameter:  
`QueueServer` will access only the two parameters it needs, and will not need to be concerned with any additional parameters that may have been delivered via the event. In this case, the default implementation of the `getSubQ` service will simply be executed. For example, the default implementation may be that the specified sub-queue is extracted from the queue. It is, of course, possible that this will not match the `QueueClient`'s expectation of `getSubQ`'s behavior, if the value of `remove` is set to false. This issue will be further discussed below in the context of behavioral inconsistency.
3. Unless this system's architectural description explicitly specifies that `Queue` is a subtype of `FIFOQueue`, or that they are identical types, `ProvInt2` will not be able to service the `ReqInt` request.

Therefore, determining whether there exists an interface inconsistency in a system will depend on several factors. At the same time, this is an architecture analysis task that can be accomplished relatively easily and should be readily automatable.

#### **Behavioral Inconsistency**

*Behavioral* inconsistencies occur between components that request and provide services whose names and interfaces match, but whose behaviors do not. As a very simple example, consider the service exported by the following interface:

```
subtract(Integer x, Integer y) returns Integer;
```

This service takes two integers as its input and returns their difference. It is natural to assume that the subtraction is arithmetic, and many math

libraries will support this as well as much more complex operations. However, the component providing this service need not calculate the two numbers' arithmetic difference. Instead, it may provide a calendar subtraction operation. Thus, for example, the requesting component may expect that the difference between 427 and 27 will be 400, while the component providing the service may treat it as the subtraction of 27 days from April 27<sup>th</sup>, and return 331 (March 31<sup>st</sup>).

An architectural model may provide a behavioral specification for the given system's components and their services. The behavioral specifications may take different forms, as illustrated in Chapter 6. For example, each required and provided interface can be accompanied with preconditions, which must hold true before the functionality exported via the interface is accessed, and postconditions, which must hold true after the functionality is exercised.

For example, let us assume that the above discussed `QueueClient` component requires a `front` operation, whose purpose is to return the first element of the queue. Furthermore, let us assume that `QueueServer` provides this operation, and that the two corresponding interfaces match. `QueueClient`'s required service behavior is specified as follows:

```
precondition q.size ≥ 0;
postcondition ~q.size = q.size;
```

where `~` denotes the value of the variable `q` after the operation has been executed. Therefore, the `QueueClient` component assumes that the queue may be empty and that the `front` operation will not alter the queue.

Let us assume that the `QueueServer` component's provided `front` operation has the following pre- and postconditions:

```
precondition q.size ≥ 1;
postcondition ~q.size = q.size - 1;
```

The precondition asserts that the queue will be non-empty, while the postcondition specifies that the operation will alter the size of the queue (i.e., that the front element will be de-queued).

A casual analysis of the two specifications indicates that the behavior of the `front` operation required by `QueueClient` does not match that provided by `QueueServer`: the postconditions clearly are different; moreover, the provided operation assumes that `front` will not be invoked before the existence of at least one element in the queue is ascertained.

A component's behavior may be specified in several different ways. Chapter 6 discussed several examples, including state-transition diagrams,

communicating sequential processes, and partially ordered events sets. The exact manner in which the behavioral consistency between services is ensured will vary across these notations, and hence is outside the scope of this text. On the other hand, the overall analysis process will follow the general pattern outlined above, regardless of the behavior modeling notation.

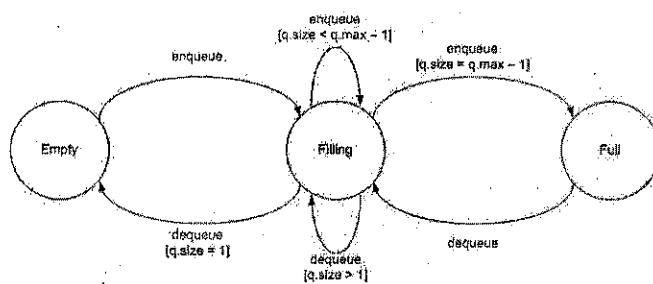
#### Interaction Inconsistency

*Interaction* inconsistencies can occur even if two components' respective provided and required operations have consistent names, interfaces, and behaviors. An interaction inconsistency occurs when a component's provided operations are accessed in a manner that violates certain interaction constraints, such as the order in which the component's operations are to be accessed. Such constraints comprise the component's interaction *protocol*.

A component's interaction protocol can be specified using different notations. Frequently, it is modeled via state-transition diagrams [306]. Analyzing the system for interaction consistency in that case consists of ensuring that a given sequence of operation requests matches some sequence of legal state transitions specified by each component's protocol.

An example such interaction protocol is provided in Figure 8-3. In the figure, the *QueueServer* component requires that at least one element always be queued before an attempt to de-queue an element can be made; furthermore, it assumes that no attempts to queue elements onto a full queue will be made. A *QueueClient* component that does not adhere to these constraints—that is, whose sequence of invocations cannot be executed by the state machine from Figure 8-3—will cause an interaction inconsistency with the *QueueServer*.

Figure 8-3. Interaction protocol for the *QueueServer* component. Transitions corresponding to operations such as *front* and *is\_empty*, typically provided by a queue component, have been elided for clarity. Transition guards are enclosed within brackets. The assumption is that the queue can contain at least two elements.



#### Refinement Inconsistency

*Refinement* inconsistencies stem from the fact that a system's architecture is frequently captured at multiple levels of abstraction. For example, a very high level model of the architecture may only represent the major subsystems and their dependencies, while a lower level model may elaborate on many details of those subsystems and dependencies. As an illustrative example, Figure 8-4 shows the high-level architecture of the Linux operating system, provided by Bowman et al. [26], and its *Process Scheduler* subsystem modeled as a composite connector, provided by Mehta et al. [191]. Analyzing Linux's architecture for completeness would need to establish the following three conditions:

1. The elements of the higher-level architectural model have been carried over to the lower-level model—that is, no existing architectural elements have been lost in the course of the refinement.
2. The key properties of the higher-level model have been preserved in the lower-level model—that is, no existing architectural design decisions have been omitted, inadvertently changed, or violated in the course of the refinement.
3. The newly introduced details in the lower-level model are consistent with the existing details of the lower-level model—that is, none of the new design decisions inadvertently change or violate the existing design decisions.

The reader should observe that Figure 8-4 does not contain enough information to establish the above three conditions. This is because both the higher-level and the lower-level models are incomplete. The one observation that can be made with certainty is that the Linux *Process Scheduler* has been maintained as a separate entity between the two refinement levels. However, at the lower level it is modeled as a connector, while at the higher level it was a component. Further analysis, and additional information on which to base that analysis, would be required before any specific determination can be made as to whether this decision—to change a component into a connector—violated any higher level architectural design decisions, and what impact it had on the rest of the architecture.

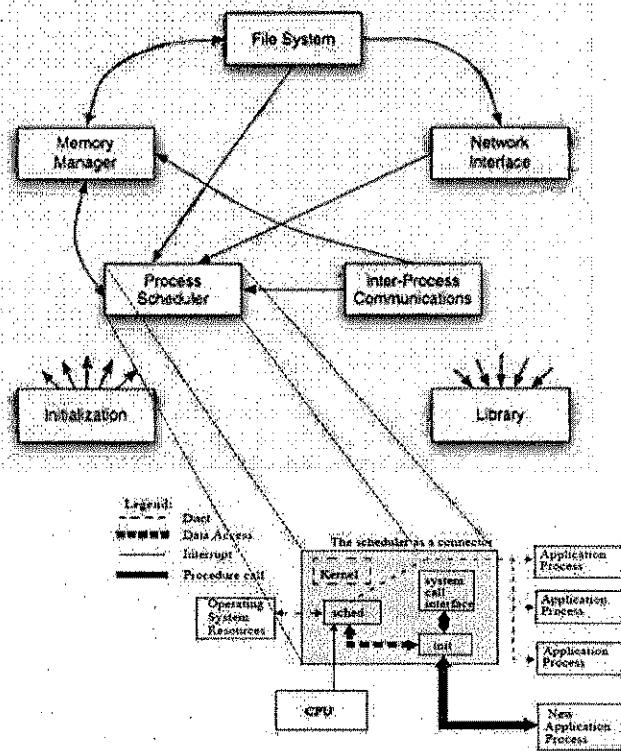


Figure 8-4. A very high-level model of the Linux operating system (adopted from Holt et al.[26]) and a detailed model of the Linux process scheduler connector.

### 8.1.3 Compatibility

Compatibility is an external property of an architectural model, intended to ensure that the model adheres to the design guidelines and constraints imposed by an architectural style, a reference architecture, or an architectural standard. If the design constraints are captured formally, or at least rigorously, ensuring an architecture's compatibility to them will be relatively straightforward. If an architecture must be compatible with a set of semi-formally or informally specified design guidelines, analyzing the architecture for compatibility may be more challenging and the outcome of the analysis process even ambiguous at times.

Reference architectures are usually specified formally, using an architecture description language. Therefore, establishing the

compatibility of a given system's architecture to the reference architecture may be a precise and automatable process. Since a reference architecture captures a set of properties that must hold true across any number of systems in a given domain, it may be only partially specified or certain parts of it may be at a very high level of abstraction. In such cases, establishing that a product-specific architecture adheres to the reference architecture can be accomplished by ensuring refinement consistency, in the manner discussed above.

On the other hand, as the reader will recall from Chapter 4, and will see further in later chapters, most architectural styles and many standards provide general, high-level design guidelines, so that establishing an architecture's adherence to them may be more challenging. The difficulty may arise from fuzziness on the part of the style definition, or imprecision or incompleteness on the part of the architectural model. For example, Figure 8-5 depicts the Lunar Lander architecture according to the event-based style. This diagram was first shown in Chapter 4, as were the relatively similar diagrams for the Lunar Lander architectures in the C2 (Figure 4-23) and blackboard (Figure 4-16) styles. Determining the style to which this architecture adheres is a non-trivial task: the depicted configuration of components may in fact also adhere to C2's principles, such as substrate independence. Likewise, this particular visual layout of the architecture's topology may be misleading, for the *SpaceCraft* component may in fact play the role of a blackboard in this system. In cases such as this, the architect may need to obtain additional information, rely on tacit knowledge, and use one or more architectural analysis techniques presented later in this chapter.

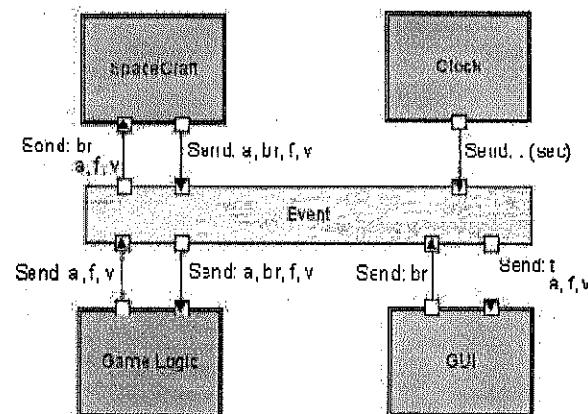


Figure 8-5. A depiction of the Lunar Lander architecture according to the event-based style.

### 8.1.4 Correctness

Correctness is an external property of an architectural model. A system's architecture is said to be correct with respect to an external system specification if the architectural design decisions fully realize those specifications. Furthermore, the system's implementation is correct with respect to the system's architecture if the implementation fully captures and realizes all the principal design decisions comprising the architecture. Correctness is therefore *relative*, comparing the architecture to some other artifact, and with respect to *elaboration* (or fulfillment), where the artifact either is intended to fulfill the architecture, or the architecture is intended to fulfill the specification.

An interesting observation arises in the implementation of many large, modern software systems that reuse off-the-shelf (OTS) functionality, or OTS architectural solutions such as reference architectures. In such cases, it is very likely that, through the OTS components, the implemented system will include structural elements or functionality, as well as non-functional properties, that are not specified in the requirements and/or not modeled in the architecture. With a 1970's notion of *refinement-based correctness*, such systems would not be considered to be correct with respect to the architecture. However, with the notion of correctness built upon fulfillment, as described above, such systems are not only correct, but they are likely efficiently created and a suitable basis for efficiently fulfilling new system requirements.

## 8.2 Scope of Analysis

A software system's architecture can be analyzed from different perspectives and at different levels. Architects may be interested in assessing the properties of individual components or connectors, or even their constituent elements, such as interfaces or ports. More frequently, architects may be interested in the properties exhibited by compositions of components and connectors in a given subsystem or entire system. A specific focus of (sub)system-level analysis may be on the data exchanged among the system elements.

In addition to assessing the properties of a single architecture, architects may at times need to consider two or more architectures simultaneously. One such case is when a given system's architecture is analyzed at multiple levels of abstraction. For example, a more detailed architectural model may be compared to the higher-level model from which it has been derived, to ensure that no existing design decisions have been violated or unintended design decisions introduced. A similar type of analysis takes place when two architectural models at similar levels of abstraction are

compared to establish design similarities or conformance to constraints such as those embodied in a reference architecture.

These different analysis targets are discussed in more detail next.

### 8.2.1 Component- and Connector-Level Analysis

While in a large system individual components and connectors may not always be as interesting to an architect as their compositions, both components and connectors need to provide specific services at specific quality levels. In the case of components this typically means application-specific functionality, while in the case of connectors this means application-independent interaction services.

The simplest type of component- and connector-level analysis is to ensure that the given component or connector provides the services expected of it. For example, a component's or connector's interface can be inspected to make sure that no expected services are missing. As an illustration, Figure 8-6 shows Lunar Lander's *Data Store* component modeled in xADL. It is trivial to analyze this component, either manually or automatically, to establish that it provides both *getValues* and *storeValues* services; furthermore, if a system stakeholder expects or requires the *Data Store* component to provide further services, he can easily ascertain that no such services currently exist. Even if the component were much larger and provided many more services, this task would not be significantly harder.

```
component{
    id = "datastore";
    description = "Data Store";
    interface{
        id = "datastore.getValues";
        description = "Data Store Get Values Interface";
        direction = "in";
    }
    interface{
        id = "datastore.storeValues";
        description = "Data Store Store Values Interface";
        direction = "in";
    }
}
```

Figure 8-6. Lunar Lander's *Data Store* component modeled in xADL. This model is extracted from that provided in Figure 26 in Chapter 6.

Of course, “checking off” the services a component or connector provides does not ensure that those services are modeled correctly. The described analysis can be thought of as equivalent to establishing only name consistency, discussed in the previous subsection. A component or connector may provide services with the expected names, but with incorrect interfaces. For example, *getValues* in the above example may be modeled to expect the values in a wrong format, such as untyped versus

typed or string versus integer. Therefore, it is not sufficient to establish that the component or connector provides appropriately named services; the complete interface of the component or connector will have to be analyzed. The information provided in Figure 8-6 will thus have to be supplemented with additional details, possibly from other models. The relevant issues in ensuring interface conformance were discussed in the previous subsection.

Taking this argument a step further, it is not sufficient to ensure that the component's or connector's services are exported via an appropriate interface. The semantics of those services as modeled (and, eventually, as implemented) may be different from the desired semantics. Thus, for example, the *getValues* service from Figure 8-6 may not be modeled such that it accesses the *Data Store* to obtain the needed values, but instead may request those values from a system user. Since the intended usage of the component, implied in its name, is to access a repository, this implementation of *getValues*, while legitimate in principle, would be wrong for this context.

Similarly, a connector may provide interaction services with semantics that are different from the expected semantics. For example, a connector may be expected to support asynchronous invocation semantics, but is actually modeled for synchronous invocation. Establishing this type of semantic consistency is not trivial. Consider as an illustration a model of a *Pipe* connector in the Wright ADL discussed in Chapter 6. The model is depicted in Figure 8-7. The *Pipe* connector plays two roles; that is, it provides two services: *Reader* and *Writer*. Their interplay, i.e., the connector's overall behavior, is captured by the connector's *glue*. Even though a pipe is a relatively simple connector, establishing manually that it adheres to its expected behavior is significantly more challenging than with name or interface conformance. For example, is the intended semantics of the pipe to allow unimpeded writing to the pipe, as in the current specification of the *writer* role, or does the pipe have a bounded buffer so that writing a certain amount of data would require that at least some of that data be read before additional data can be written? Assessing more complex connectors for these types interaction properties will be much more difficult and may be especially error prone.

Figure 8-7. Pipe connector modeled in Wright.

```

connector Pipe ==
  role Writer = write → Writer []
    close → ✓
  role Reader =
    let ExitOnly = close → ✓
    in DoRead = (read → Reader []
      read-eof → ExitOnly)
    in DoRead [] ExitOnly
  glue = let ReadOnly = Reader.read → ReadOnly []
    Reader.read-eof → Reader.close → ✓ []
    Reader.close → ✓
    in let WriteOnly = Writer.write → WriteOnly []
      Writer.close → ✓
    in Writer.write → glue []
      Reader.read → glue []
      Writer.close → ReadOnly []
      Reader.close → WriteOnly
  
```

## 8.2.2 Subsystem- and System-Level Analysis

Even if individual components and connectors have desired properties, no guarantees can be made that their compositions in a given system will behave as expected, or even be legal. The interplay among complex components can itself be very complex. Architects may assess the properties of their compositions at the level of the entire system or incrementally, by focusing on particular subsystems.

The most manageable increment is pair-wise conformance, where only two interacting components are considered at a time, and name, interface, behavior, and interaction conformance are established as discussed above. The next step up is to take a set of components possibly interacting through a single connector, such as those shown in Figure 8-5. Most analysis techniques can easily support both these cases. Ensuring desirable properties at the level of large subsystems and entire systems can be quite challenging, and many analysis techniques have tried to get a handle on this problem.

In certain scenarios it may be obvious that compositions of two or more components that respectively possess properties  $\alpha$ ,  $\beta$ ,  $\gamma$ , etc. will have some combination of those properties. For example, combining a data encryption component—intended to provide communication security—with a data compression component—intended to provide communication efficiency—can be expected to provide both security and efficiency.

Much more frequent in practice is the situation where the interplay among the components will result in their interference, and either enhancement or diminishment of each other's properties. This will be acceptable, and even desirable, in certain cases. For example, a component that provides a

critical service very efficiently may be vulnerable to malicious attacks. The system architects may decide that sacrificing some of the efficiency is acceptable in order to enhance the system's security, and may compose this component with one or more components that provide services such as encryption, authentication, or authorization. Likewise, in many real-time systems, a component that computes its results or provides data more quickly and/or frequently than the system requires will be composed with a (simple) component that introduces the necessary delays. Such compositions will be synergistic: the system will ultimately be greater than the sum of its parts.

Such interference among system components will not be desirable in all situations. More importantly, such interference will often not be as obvious as in the above scenarios and will result in unintended composite properties. Examples abound. One such well known example from software engineering literature involved integrating two components which both assumed that they own the system's main thread of control, ultimately resulting in an unusable system [88]. Another similar example involved integrating concurrent components implemented in two different programming languages. The resulting system's performance was unacceptable, and a long and painstaking analysis of the system uncovered that the individual components' threading models were incompatible [187]. The reader can easily envision many other such scenarios, such as when a system comprises interacting memory-efficient components (which use computationally intensive data compression algorithms) and CPU-efficient components (which use techniques such as data caching and pre-fetching) or, further, when a component introducing a fault-tolerance service (e.g., via continuous state replication) is introduced into such a system.

Scenarios such as those discussed in this section are the direct reason why many modern software systems suffer from poor performance, security, and scalability; unnecessarily large size; high complexity; limited adaptability; and so on (these properties will be further discussed in Chapters 12 and 13). For example, a concurrent system in which any component or subsystem considered in isolation is deadlock-, livelock-, and starvation-free may in fact suffer from deadlock, livelock, or starvation because of the unforeseen interplay of multiple components and/or subsystems.

This is what Dewayne Perry has colloquially referred to as the *honey-baked ham* syndrome: honey is fat-free, while ham is sugar-free; honey-baked ham, therefore, must be both fat-free and sugar-free. Clearly, this is not true, and drawing such conclusions based on the evidence available

from a system's individual components may be wrong and perilous. The *honey-baked ham* syndrome is the primary reason why subsystem- and system-level architectural analysis is critically important.

### 8.2.3 Data Exchanged in the System or Subsystem

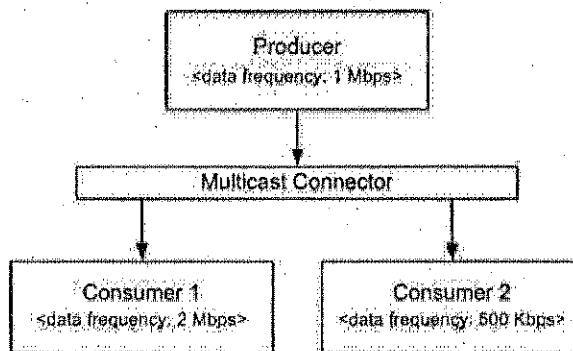
In many large, distributed software systems large amounts of data are processed, exchanged, and stored. Examples of data-intensive systems are numerous and appear in such wide ranging domains as scientific computing, many Web-based applications, e-commerce, and multimedia. In such systems, in addition to the properties of the individual structural architectural elements—components and connectors—and the entire architectural configuration, it is important to ensure that the system's data is properly modeled, implemented, and exchanged among the structural elements. This involves ensuring the intended

- structure of the data, such as typed versus untyped or discrete versus streamed,
- flow of the data through the system, such as point-to-point versus broadcast, and
- properties of data exchange, such as consistency, security, and latency.

As a simple example, consider a system consisting of a data producer component and two data consumer components, whose architectural configuration is depicted in Figure 8-8. The figure also shows the respective frequencies at which they are able to exchange data. The *Producer* component sends one megabit per second, and *Consumer 1* is able to receive and process that data in a timely manner. In fact, *Consumer 1* may wait idly up to 50% of the time to receive additional data from the *Producer*. On the other hand, *Consumer 2* is able to receive and process the data at a rate that is only one half of the production rate. This means that *Consumer 2* may lose up to one half of the produced data.

This problem may be mitigated if the *Multicast Connector* servicing the three components is able to buffer data, but clearly, if the system is long running, the connector's buffer will quickly overflow. Additionally, the connector will have to include additional processing logic to store the data temporarily and also route it to the two components in the order received, which will introduce additional overhead in the system. If the two *Consumer* components require the data to be in different formats from that generated by the *Producer*, the connector will also have to act as an adapter, introducing further overhead. Likewise, the connector may have to perform additional tasks based on the architectural requirements, such as encrypting the data for security, ensuring that the data is delivered

according to the specified routing policy (e.g., best effort or exactly once), or compressing the data if necessary.



**Figure 8-8.** A simple system with one data producer and two consumers, with the frequencies at which they are able to send and receive data, respectively.

#### 8.2.4 Architectures at Different Abstraction Levels

During the architectural design process, architects will frequently address the critical system requirements first, and then both introduce additional elements into the architecture and refine the architecture to include additional details that are necessary for the architecture's realization into the final system. This may involve the addition and further breakdown of architectural elements, as well as the introduction and refinement of existing design decisions.

Consider a simple example. A high-level architectural breakdown of a system may look like the diagram shown in Figure 8-9. For simplicity, the connectors are depicted only as arrows indicating the interacting components as well as the direction of interaction. For example, component *C1* initiates the interactions with components *C3* and *C4*. As is the case with all boxes-and-arrows architectural descriptions, many details of this architecture are missing, including the components' interfaces, details of their behaviors and of the data exchanged, as well as the semantics of their interactions, such as that involving components *C1*, *C2*, and *C3*. While important, such information is not critical to this discussion.

**Figure 8-9.** A high-level architectural configuration.

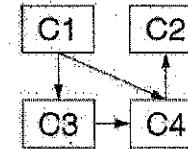
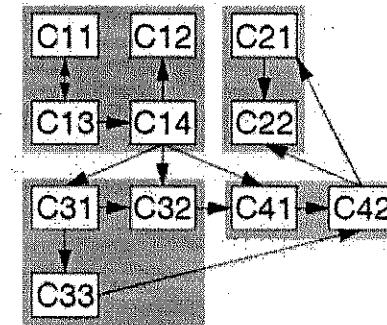


Figure 8-10 depicts another architectural configuration, which is intended to be a refinement of that shown in Figure 8-9. For convenience, groups of components in the refined architecture which are presumed to comprise the original components are highlighted. For example, components *C11*, *C12*, *C13*, and *C14* along with their interconnections in Figure 8-10 comprise component *C1* from Figure 8-9. Furthermore, the connectors are refined, such that it is clear that only *C1*'s subcomponent *C14* is engaged in interactions with the subcomponents of *C3* and *C4*.

**Figure 8-10.** A refined, more detailed architectural configuration.



In the process of refinement, several problems can be introduced, as discussed above in the context of refinement incompatibility. The easiest cases to address are those where an architectural design decision has been clearly invalidated. However, even the addition or modification of architectural decisions may cause a refinement inconsistency depending on the context and on the range of architectural changes that are allowed. For example, the architecture depicted in Figure 8-9 and Figure 8-10 may need to abide by an architectural constraint stating that interactions crossing the boundaries of the system's original four components must have a single target and a single destination. In that case, elaborating the interactions among the architecture's components as shown in Figure 8-10

would violate the constraints, both in the case of component  $C_1$ 's interactions with  $C_3$  and  $C_4$ 's interactions with  $C_2$ .

Clearly, based on the scant information provided about the architectures in Figure 8-9, it is unclear whether the changes to the original architecture depicted in Figure 8-10 should be allowed. This will depend on many factors, some though not all of which will be apparent from a more detailed and rigorous modeling of the architecture such as those discussed in Chapter 6. This will also depend on a refinement policy, which may be explicitly stated. Thus, for example, Moriconi and colleagues define a refinement policy called *conservative extension* [197]. Conservative extension essentially precludes an architect from introducing any new features into a system's architecture, and instead restricts him to either elaborating or possibly eliminating those features already existing in the more abstract, i.e., higher level, architecture. While a property such as conservative extension may not always be useful in practice, Moriconi and colleagues have shown it to be amenable to formal specification and analysis. Other refinement policies may be much less restrictive, but that very flexibility may make it difficult to establish that they are being adhered to in a concrete situation.

### 8.2.5 Comparison of Two or More Architectures

In certain situations it is important for architects to understand the relationship between the architecture they are interested in and a baseline architecture with known properties. One such case, discussed previously in this chapter, is ensuring the compliance of a given system's architecture with a reference architecture. Other cases may include ensuring the architecture's compliance with the design guidelines captured in an architectural style or with a particular design pattern. It is, of course, also possible that the baseline architecture is simply one that the architect is familiar with and understands its properties. The architect may have encountered this architecture in literature, it may be the architecture of a related product he and his colleagues had developed previously, or it could even be an architecture that has been recovered from a system (possibly even competitor's system) that exhibits desired properties.

Such comparisons of two or more architectures involve comparing the processing and data storage capabilities provided by the components, the interactions as embodied in the connectors, the characteristics of the data exchange, the components' and connectors' compositions into the system's configuration, and the sources of the non-functional properties exhibited by the system. It is possible for the architectures in question to be at different levels of abstraction, in which case the techniques discussed in the previous subsection can be employed.

## 8.3 Architectural Concern Being Analyzed

Architectural analysis techniques are directed at different facets of a given architecture. Some techniques strive to ensure primarily the architecture's *structural* properties; others focus on the *behaviors* provided by the architectural elements and their composition; yet others may analyze whether the *interactions* among the architectural elements adhere to certain requirements and constraints; finally, the *non-functional properties* exhibited by the architecture are frequently considered to be very important and are thus studied carefully.

In practice, a given analysis technique, or suite of techniques, will address more than one architectural concern at a time. In this section we will focus on each concern individually for ease of exposition, and discuss their relevant characteristics.

### 8.3.1 Structural Characteristics

The structural characteristics of a software architecture include concerns such as the connectivity among an architecture's components and connectors, containment of lower-level architectural elements into composite higher-level elements, possible points of network distribution, and a given system's potential deployment architectures. These concerns can help to determine whether the architecture is well formed. Examples include components or subsystems that are disconnected from the rest of the architecture, missing pathways between components and connectors that are intended to interact, existing pathways between components and connectors that are not, encapsulation of components or connectors that must be visible and accessible at a higher level of hierarchical composition, and so on. Structural analysis can also establish adherence to architectural constraints, patterns, and styles. Structural concerns can also help in the analysis of different aspects of system concurrency and distribution, as they tie the system's software elements and their properties with the hardware platforms on which they will execute.

#### Behavioral Characteristics

A well structured architecture is of limited utility if the individual components do not provide the behaviors that are expected of them and, further, if they do not combine to provide the expected system-level behaviors. Therefore, analyzing an architecture's behavioral characteristics has two related facets:

1. considering the internal behaviors of individual components, and
2. considering the architectural structure to assess composite behaviors.

It is possible, especially in systems composed with third-party components obtained off-the-shelf, that an architect's insight into the internal workings

of different system components will be restricted to the components' public interfaces. As indicated above, particularly in Section 8.1, the types of behavioral properties that can be inferred at the level of interfaces are quite limited, and many potential problems with the architecture may remain undetected.

#### **Interaction Characteristics**

The relevant characteristics of interactions in a given architecture may include the numbers and types of distinct software connectors, and their values for different connector dimensions (recall Chapter 5). Interaction characteristics can help to establish whether the architecture will actually be able to fulfill some of its requirements. For example, a non-buffering connector in the example from Figure 8-8 would result in a system in which one of the components received at most one half of all the data.

Analysis of interaction characteristics may also encompass the interaction protocols for different system components (for example, recall Figure 8-3) and internal behaviors specified for different system connectors (for example, recall Figure 8-7). Such details would aid in the analysis of finer-grain interaction characteristics, such as whether a component interacting through an otherwise appropriate connector will be legally accessed, or whether a set of interacting components may deadlock.

#### **Non-Functional Characteristics**

Non-functional characteristics form a critical dimension of almost all software systems. These characteristics typically cut across multiple components and connectors, which makes them particularly difficult to assess. Furthermore, non-functional characteristics are often not properly understood, they are qualitative in nature, and their definitions are partial or informal. Therefore, while the non-functional characteristics present an important and formidable challenge to software architects, architectural analysis techniques focusing on these characteristics are scarce.

### **8.4 Level of Formality of Architectural Models**

The relationship between architectural models and analysis is symbiotic: what the system's stakeholders want to be able to analyze will influence what software architects capture in their architectural models. Conversely, what architects capture in the architectural models directly determines what they will be able to analyze and what analysis methods they will use to do so.

Architectural models have been discussed in detail in the preceding chapters, and particularly in Chapter 6. Here we will look specifically at the role they play in the context of architectural analysis. For that purpose, architectural models can be classified as informal, semi-formal, and formal.

#### **Informal Models**

Informal models are typically captured in boxes-and-lines diagrams such as that shown in Figure 8-1. Informal models can provide a useful high-level picture of the system. They are amenable to informal and manual analyses, typically by a broad section of stakeholders, including non-technical stakeholders such as managers and system customers. For example, system managers can use them to determine a project's overall staffing needs. At the same time, informal models should be approached cautiously because of their inherent ambiguity and lack of detail.

#### **Semi-Formal Models**

Most architectural models used in practice are semi-formal. A notation that strives to be useful to a large number of system stakeholders, both technical and non-technical, will typically try to strike a balance between a high degree of precision and formality on the one hand, and expressiveness and understandability on the other. One widely used example the reader will recall from Chapter 6 is the Unified Modeling Language (UML). Semi-formal languages such as the UML are amenable both to manual and automated analysis. Their partial imprecision makes it difficult to perform some more sophisticated analyses, for which formal models are needed.

#### **Formal Models**

While semi-formal modeling notations typically only have a formally defined syntax, formal notations also have formally defined semantics. An example formal notation is Wright, which was used to specify the *Pipe* connector in Figure 8-7. Formal models are inherently amenable to formal, automated analysis and are typically intended for the system's technical stakeholders. At the same time, producing complete architectural models using a formal notation can be painstaking. Furthermore, formal models have been frequently shown in practice to suffer from scalability problems.

### **8.5 Type of Analysis**

One useful categorization of architectural analysis techniques is into static, dynamic, or scenario-based techniques. We discuss the three categories and the role architectural models play in each.

#### **Static Analysis**

Static analysis involves inferring the properties of a software system from one or more of its models, without actually executing those models. A simple example of static analysis is syntactic analysis: determining if the system model adheres to the syntactic rules of the modeling notation, whether it be an architectural description language, design diagramming notation, or programming language. Static analysis can be automated (e.g., compilation) or manual (e.g., inspection). All architectural modeling

notations, including the informal boxes-and-lines diagrams, are amenable to static analysis, although naturally, the more formal and expressive notations can be harnessed to provide more precise and sophisticated answers. Formal notations used in modeling software systems include

- axiomatic notations, which model systems via logical assertions – an example is Anna [169],
- algebraic notations, which model systems via collections of equivalence relations – an example is LARCH [106], and
- temporal logic notations, which model systems in terms of order of execution and timing – an example is GIL [64].

It should be noted that the above example notations cannot be considered as architecture description languages, or ADLs, since by themselves, they do not provide any explicit architecture modeling constructs. However, it is possible to use them as a basis of an ADL, much in the same way that Wright leverages CSP as discussed in Chapter 6.

#### **Dynamic Analysis**

Dynamic analysis involves actually executing or simulating the execution of a model of the software system. In order to perform dynamic analysis on an architectural model, its semantic underpinning must be executable or amenable to simulation. State-transition diagrams are an example executable formalism with which the reader should be familiar. Other example executable formalisms include discrete events, queuing networks [162], and Petri nets.

#### **Scenario-Based Analysis**

For large and complex software systems, it is often infeasible to assert a given property for the entire system over the entire space of its possible states or executions. For such systems, specific use cases are identified that represent the most important or most frequently occurring system usage scenarios, and the analysis is focused on those. Scenario-based analysis can be an instance of both static analysis –as a tool for reducing a modeled system’s state space, as discussed later in this chapter– and dynamic analysis –as a tool for reducing the system’s execution space. At the same time, scenario-based analysis requires that architects be very careful about the inferences they make from their inherently limited evidence.

## **8.6 Level of Automation**

Different architectural analysis techniques are amenable to different levels of automation. The level of automation depends on several factors, including the formality and completeness of the architectural model, and the property being assessed. In general, an architectural model provided in a more formal notation will be more amenable to automated analysis than a model provided in a more informal notation. Likewise, a model that captures a greater number of the architectural design decisions for the

given system will be more amenable to rigorous, automated analysis than a model that is missing many such design decisions. Finally, a well understood property that is quantifiable and can itself be defined formally will be easier to assess automatically than a qualitative property that may not be as well understood. This last point is particularly important in software engineering: as will be demonstrated in Chapter 12, many non-functional properties, which are critical to the success of most all software systems, are understood at the level of intuition, anecdote, and informal guideline.

#### **Manual**

Manual analysis of software architectures requires significant human involvement, and is thus expensive. However, manual analysis can be performed on models of varying levels of detail, rigor, formality, and completeness. It has the added advantage that architectural rationale, which is often tacit, can be taken into account. This type of analysis may also be required when multiple, potentially clashing properties must be ensured in tandem.

A number of architectural analysis techniques fall in this category. These are inspection-based techniques and will be further elaborated upon in the next section. One well known example is the architecture trade-off analysis method, or ATAM [39]. The analysis results emerging from manual analysis are typically qualitative. Since it is not always possible to quantify important properties of a software system –such as scalability, adaptability, or heterogeneity– any analysis of the extent to which the system exhibits those properties will not be quantifiable. The analysis results are also frequently qualified by a particular context in which a system may exhibit a given property. Scenario-based techniques fall in this category.

Given the human-intensive nature of this category of architecture analysis techniques, a critical concern must be to make the analysis reliable and repeatable. Since the architectural models as well as the properties of interest may be less than formally captured, the focus of many manual analysis techniques has been on specifying a detailed process that must be followed by the system architects and other stakeholders participating in the analysis.

#### **Partially Automated**

Growing levels of rigor in architectural models, and in understanding of the software systems’ key properties, present opportunities for automating different facets of architectural analysis. In fact, most architectural analyses can be at least partially automated, involving both software tools and human intervention. In that sense, architectural analysis techniques can be thought of as covering a spectrum of automation, with manual and full analysis being the ends of that spectrum.

Most architecture modeling notations presented in Chapter 6 are amenable to ensuring a given architectural description's syntactic correctness, as well as different degrees of semantic correctness. For example, a xADL model can be analyzed for style-specific component interconnectivity rules, while Wright allows one to analyze a given composition of components communicating through a connector for deadlocks. At the same time, neither model can be analyzed automatically for other properties, such as reliability, availability, dependability, or latency. This is at least in part because system parameters that are relevant to assessing these properties are not captured—to the necessary degree, or at all—by these architectural modeling notations.

#### Fully Automated

It can be argued that the specific analyses mentioned above, such as ensuring the syntactic correctness or deadlock freedom in an architectural description, can be considered fully automatable since it is possible to complete them without human involvement. At the same time, the results of automated analyses are typically partial: the fact that an architectural description provided in a given ADL fully adheres to that ADL's syntax, or that a partial system description provided is deadlock free, still leaves a large number of questions about the respective models unanswered. This means that, in practice, fully automated architectural analysis techniques must be combined with other techniques, which themselves may need human intervention, in order to get more comprehensive answers.

## 8.7 System Stakeholders

The stakeholders in a software project will often have different objectives. For example, customers may be interested in getting the most functionality as quickly as possible, for the lowest amount of money possible. A project manager may be interested in ensuring that the project is staffed appropriately and that the “burn rate” does not exceed some target. The architects' primary objective may be to deliver a technically sound system that will be easily adaptable in the future. Finally, a developer may be interested primarily in ensuring that the modules he is tasked with are implemented on time and bug-free. Therefore, the different stakeholders will not necessarily have identical architecture analysis needs. The remainder of this section highlights the role architectural analysis plays in the case of each stakeholder type.

#### Architects

Software architects must take a global view of the architecture and are interested in establishing all four “C’s” in the architecture: completeness, consistency, compatibility, and correctness. Depending on the project's context and objectives, architects may need to rely on all types of architectural models at all levels of scope and formality. While they may

prefer to use automated analysis techniques, architects will frequently have to rely on manual and semi-automated techniques.

#### Developers

Software developers often take a more limited view of the architecture—namely, the modules or subsystems for which they are directly responsible. As such, developers are interested primarily in establishing the consistency of their modules with other parts of the system with which these modules will interact, as well as compatibility with the required architectural styles, reference architectures, and standards. They need not worry about the architecture's completeness, and can at best assess its partial correctness. The models that developers will likely find most useful are formal, with all necessary details specified and ready for implementation. However, these would likely be models of individual elements for which a given developer is directly responsible, rather than models of the entire architecture.

#### Managers

Project managers are typically primarily interested in an architecture's completeness—*are all the requirements satisfied*—and correctness—*are the requirements appropriately realized in the architecture*, and eventually in the implementation. Managers may also be interested in the architecture's compatibility if the architecture, and eventually the implemented system, has to adhere to a reference architecture or a set of standards.

Consistency is a system's internal property, and managers typically do not concern themselves with it, i.e., they naturally delegate such responsibilities to architects and developers. There are exceptions, however. For example, architectural defects may become a major issue that begins affecting the project's schedule or budget. Alternatively, customers or project contracts may explicitly mandate certain consistency properties, in which case managers would need to explicitly consider them.

The types of architectural models that are useful to managers are usually less formal models of the entire system. A manager's focus will frequently be on cross-cutting non-functional system properties, as well as the system's structural and dynamic characteristics.

#### Customers

Customers are interested primarily in the commissioned system's completeness and correctness. Their concerns can be summarized with two key questions:

1. Is the development organization building the right system?
2. Is the development organization building the system right?

A customer may also be interested in the system's compatibility with certain standards, and possibly reference architectures in which the

customer has a vested interest. Consistency is not of critical importance unless it is reflected in externally visible system defects.

In terms of architectural models, customers typically favor understandability over formality of models. They are interested in overall models (the “big picture”) and the system’s key properties. They are often interested in scenario-driven assessment of a system’s structural, behavioral, and dynamic characteristics.

#### Vendors

Software vendors typically sell technology, such as individual components and connectors, rather than architecture. As such they are interested primarily in composability of those components and connectors as well as their compatibility with certain standards and widely used reference architectures. Like a given system’s customers, vendors may value the understandability of architectural models, but their customers are software developers who may demand formal models of the software they purchase from the vendor. The vendors’ primary focus is on the analysis of the individual elements and their properties. The structural characteristics of the overall architecture are not as important, although dynamic characteristics may be since they may have implications on the composability of the individual elements in future systems.

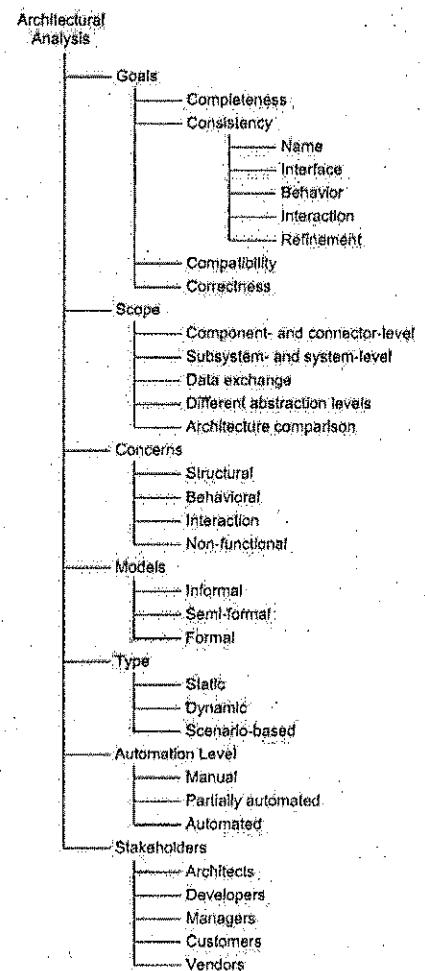
## 8.8 Analysis Techniques

A large number of analysis techniques are available to software architects. Some of them are variations on techniques applied to other software development artifacts –primarily formal specifications and code– while others have been developed specifically with software architectures in mind. In this section we will discuss a cross-section of architectural analysis techniques. Although it is not intended to provide a complete overview of existing techniques, the cross-section is broadly representative.

We divide architectural analysis techniques into three categories:

- inspection- and review-based,
- model-based, and
- simulation-based.

The discussion of the techniques within these categories will center around the architectural analysis dimensions outlined above and summarized in Figure 8-11.



**Figure 8-11.**  
Architectural analysis dimensions discussed in this chapter.

### 8.8.1 Inspections and Reviews

Software inspections and reviews are widely used code analysis techniques. If unfamiliar with these techniques, the reader is encouraged to consult an introductory software engineering text. *Architectural*

inspections and reviews are conducted by different stakeholders to ensure a variety of properties in an architecture. They involve a set of activities conducted by system stakeholders in which different architectural models are studied for specific properties. These activities often take place in architecture *review boards*, where a number of stakeholders defines the objective of the analysis –e.g., ensuring that the architecture satisfies a given non-functional property– and then, as a group, carefully studies and critiques the architecture or some of its parts.

Inspections and reviews are manual analysis techniques, and as such can be expensive. On the other hand, they have the advantage of being useful in the case of informal or partial architectural descriptions. They can also be employed effectively in the case of “soft” architectural properties, such as scalability or adaptability, which are not precisely understood and amenable to formal definition. Another advantage of inspections and reviews is that they can simultaneously take into account the objectives of multiple system stakeholders and consider multiple desired architectural properties.

Depending on the context, inspections and reviews can have any of the four architectural analysis *goals*: consistency, correctness, completeness, and compatibility. In terms of consistency, they will typically be well suited to name and interface consistency analysis. Behavior, interaction, and refinement consistency analysis may be conducted by the technical stakeholders –architects and developers– although doing so manually may be a difficult and error-prone task. For example, recall the interaction characteristics embodied in the single Wright *pipe* connector from Figure 8-7, and even the comparatively simpler single state-transition interaction protocol of the *QueueServer* component from Figure 8-3. Dealing with a large number of such models manually would cognitively overload even the most capable architects. Thus, if analyzing for any of the three latter types of consistency is undertaken during an architectural inspection or review, it may be advisable to restrict the analysis to carefully confined subsets of the architecture.

The *scope* of inspections and reviews can vary. The stakeholders may be interested in individual components and connectors, or their compositions in a specific subsystem or the entire system. The stakeholders may also center on the data exchanged among the specific components and connectors or, globally, across the entire architecture. They may try to assess the compliance of the architecture to a higher-level architecture that served as its starting point. They may also try to assess the architecture’s similarity to an existing architecture with known properties.

Similarly, the specific *concern* of the analysis can vary. The stakeholders may focus on the structural, behavioral, or interaction properties, although

as mentioned above, the latter two may be difficult to assess manually. Inspections and reviews may be particularly well suited to establishing certain non-functional properties, especially those that require some “interpretation” and consensus reaching by the human stakeholders.

In terms of the types of *models* particularly amenable to inspections and reviews, any level of formality may be suitable in principle. However, highly formal models will not be useful to the non-technical stakeholders, and even the technical stakeholders may find them difficult to read and understand. At the other end of the spectrum, informal models may be useful if, for example, the objective of the inspection is to develop a common understanding of the architecture’s general characteristics. On the other hand, it may not be very meaningful to rely on informal models when inspecting the architecture for concrete properties of interest.

By their nature, the *types* of analysis for which inspections and reviews are geared are static and scenario-based. Since the stakeholders will manually assess the architectural models, they will have to focus on the architecture’s static properties, such as proper connectivity, interface conformance between interacting components, adherence to desired architectural patterns, and so on. Furthermore, as will be discussed below in the case of the ATAM analysis technique, the stakeholders may manually run through some critical scenarios to ensure that the architecture will behave as expected.

As already mentioned, in terms of *automation level* inspections and reviews are manual, very human intensive.

Finally, all system *stakeholders*, save for perhaps component vendors, may participate in inspections and reviews. Architects and developers will conduct inspections and reviews most frequently, and will periodically be joined by project managers and possibly by customers.

In the remainder of this section we will outline a widely used architecture inspection and review technique, ATAM.

## ATAM

The Architectural Trade-off Analysis Method [CKK2002], or ATAM, developed at Carnegie Melon’s Software Engineering Institute (SEI), is a human-centric process for identifying risks in a software design early on in the development lifecycle. ATAM specifically focuses on the quality attributes, or non-functional properties (NFPs), of modifiability, security, performance, and reliability. Its objective is to reveal not only how well an architecture satisfies given quality goals, but also how those goals trade off against each other.

- The ATAM process requires the gathering of the software architects designing the system, other important stakeholders of that system, and a separate independent architecture evaluation team. An evaluation using ATAM typically takes three to four days.

The set of activities followed are depicted in Figure 8-12. The remainder of this section will elaborate on the process depicted in the figure.

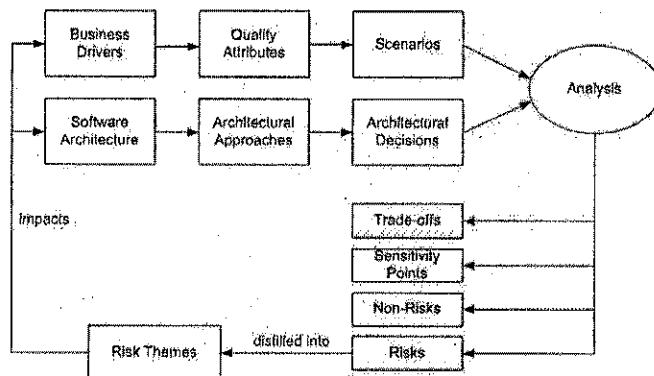


Figure 8-12. The high-level view of the process steps followed in ATAM. The diagram has been adopted from [http://www.sei.cmu.edu/architecture/ata\\_method.html](http://www.sei.cmu.edu/architecture/ata_method.html)

Two key inputs into the ATAM process are the *business drivers* and the system's *software architecture*. A project's decision maker, who is usually the project's manager or customer, first presents the system's major business drivers. These include

- the system's critical functionality,
- any technical, managerial, economic, or political constraints,
- the project's business goals and context,
- the major stakeholders, and
- the principal *quality attribute* (NFP) goals that impact and shape the architecture.

The quality attributes become a basis of eliciting a set of representative scenarios that will help ensure the system's satisfaction of those attributes. The scenarios in ATAM are divided into

- use-case scenarios, which describe how the system is envisioned by the stakeholders to be used,
- growth scenarios, which describe planned and envisioned modifications to the architecture, and
- exploratory scenarios, which try to establish the limits of architecture's adaptability by postulating major changes to the

system's functionality, operational profiles, and underlying execution platforms.

Once the scenarios are identified, they are prioritized in terms of importance by the system's stakeholders.

Another thread of activity in ATAM involves the project's architects presenting the key facets of the architecture. This includes

- technical constraints such as the required hardware platforms, operating systems, middleware, programming languages, and off-the-shelf functionality,
- any other systems with which the system under development must interact, and
- architectural approaches* that have been used to meet the quality requirements.

An architectural approach in ATAM refers to any set of architectural design decisions made to solve the problem at hand. Architectural approaches are typically architectural patterns and styles. The architectural approaches are used to elaborate the architectural design decisions made for the system.

The key step in ATAM is the *analysis* of the architectural approaches in the context of the identified scenarios, with the primary goal of establishing the relationship between the approaches—that is, architectural design decisions—and quality attributes. The analysis is not rigorous, but rather is intended to observe general, coarse-grained characteristics of the architecture. To this end, for each architectural approach a set of analysis questions are formulated that are specific to the quality attributes and architectural approach under consideration. The system's architects engage with the ATAM evaluation team in answering these questions. The answers particularly focus on the architectural approach's known risks (i.e., weaknesses), non-risks (i.e., strengths), sensitivity points, and quality trade-off points.

Depending on the architects' responses, any of the answers may be used as a starting point for further analysis. For example, let us assume that an architect is unable to answer questions about a given subsystem's event processing priorities or about the overall system's deployment—that is, the allocation of software components to hardware nodes, further discussed in Chapter 10. In that case, there will be no point in investing further resources to perform rigorous model-based or simulation-based analyses such as the construction of queueing networks or rate-monotonic performance analysis.

Finally, the risks identified in the given iteration of ATAM are distilled into *risk themes* and are fed back to the ATAM inputs of software

architecture and business driver. The objective is to repeat the above process until all major architectural risks are properly mitigated.

Regardless of its actual effectiveness, any inspection- and review-based architectural analysis process such as ATAM will sensitize a system's stakeholders to the important facets of their architecture. In ATAM's case, because of its focus and objectives, as well as the prolonged participation of system stakeholders, it has a high potential of resulting in clarified quality attribute requirements for the system, a better documented basis for architectural decisions, identification of risks early in the life-cycle, and increased communication among stakeholders.

The below table summarizes ATAM according to the architectural analysis criteria introduced in this chapter.

<b>Goals</b>	Completeness Consistency Compatibility Correctness
<b>Scope</b>	Subsystem- and system-level Data exchange
<b>Concern</b>	Non-functional
<b>Models</b>	Informal Semi-formal
<b>Type</b>	Scenario-driven
<b>Automation Level</b>	Manual
<b>Stakeholders</b>	Architects Developers Managers Customers

### 8.8.2 Model-Based Analysis

Model-based architectural analysis techniques rely solely on a system's architectural description and manipulate that description to discover properties of the architecture. Model-based techniques involve analysis tools of different levels of sophistication. These tools are frequently guided by architects, who may have to interpret the intermediate analysis results and guide the tool in further analysis.

Because of their tool-driven nature, model-based techniques are much less human intensive, and hence usually less costly, than inspections and reviews. On the other hand, they can only be used to establish "hard" properties of a system's architecture, i.e., those properties that can be

encoded in the architectural model. They cannot easily account for implicit properties — those that a human might readily infer from the existing information, and thus chooses not to model explicitly. Additionally, model-driven analysis techniques cannot typically assess "soft", but very important, aspects of an architecture, such as design intent and rationale. Model-based techniques usually also focus on a single, specific facet of a system's architecture, such as syntactic correctness, deadlock freedom, adherence to a given style, and so forth.

Another concern with model-driven analysis techniques is their scalability: more sophisticated techniques are required to keep track of a very large number of the modeled system's elements and properties. The usual trade-off encountered in many static analysis tools, of which model-based architectural analysis tools are an instance, is between scalability on the one hand and precision or confidence on the other. In other words, architects may be able to arrive at highly precise analysis results with a high degree of confidence in those results for smaller systems, but would have to sacrifice that precision and confidence for larger systems. Because of all these reasons, the results of model-driven analysis are usually partial, and multiple such techniques are used in tandem in any given architecture-driven software development project. Even then, model-based analysis usually does not provide all the needed answers to an architect, and is coupled with techniques from the other two categories—inspections and reviews, and simulation-based analysis.

The *goals* of model-based architectural analysis techniques are usually consistency, compatibility, internal completeness. The goals can also include certain aspects of external completeness and correctness. Recall that both external completeness and correctness assess the adherence of a system's architectural model to the requirements, and of the system's implementation to the architectural model. Certain facets of external completeness and correctness, such as structural completeness or correctness, can be established from the architectural model. Furthermore, the output of the analysis technique may be automatic generation of (partial) system implementation from the architectural model, which would ensure external completeness and correctness by construction. If the analysis involves system requirements, then the requirements will need to be formalized to some extent.

The *scope* of model-based architectural analysis can span individual components and connectors, their compositions in a specific subsystem or the entire system, as well as the data exchanged among the specific components and connectors or, globally, across the entire architecture. Model-based techniques may also try to assess the compliance of the model to a higher-level model from which it has been derived. Analysis techniques in this category may also try to assess the architecture's

similarity to an existing architecture with known properties. This presumes that both architectures are modeled in one of the notations supported by the analysis technique.

Similarly, the specific *concern* of model-based analysis can vary. The techniques may focus on the structural, behavioral, or interaction properties. Behavioral and interaction properties may be difficult to assess completely using model-based techniques alone, and these techniques are usually coupled with simulation-based approaches. Model-based techniques can be used to analyze an architecture's non-functional properties, but usually require the use of specific formalisms. This issue will be studied in more depth later in this section.

In terms of the types of *models* particularly amenable to this type of analysis, the general rule-of-thumb is that more formality yields more meaningful and precise results. Thus, for example, a Wright specification, such as that shown in Figure 8-2 will be much more amenable to manipulation by an analysis tool than an informal diagram such as that shown in Figure 8-1. Usually the architectural models to which sophisticated analysis tools are applied have formally specified syntax as well as semantics.

By their nature, the *type* of analysis for which model-based techniques are well suited is static analysis. These techniques are well suited to assessing properties proper connectivity, type checking, definition-use analysis of architectural services, interface and behavioral conformance between interacting components, structural adherence to desired architectural patterns, deadlock freedom, and so on.

As already mentioned, in terms of *automation level* model-based techniques are typically at least partially automated, and are often fully automated, requiring no human intervention.

Finally, model-driven architecture analysis techniques are usually targeted at the technical *stakeholders*, namely architects and developers. Other stakeholders may be interested in summaries of analysis results, but typically these techniques require a certain degree of mastery and provide low-level insights into the architecture.

The remainder of this section will first survey the spectrum of model-based analysis techniques developed for different architecture description languages, and will then discuss how architectural models can be leveraged to enable analysis of a representative non-functional property—reliability.

A particular, widely used model-based analysis technique in computer-based systems (software as well as hardware) is model checking. Model checking is a method for algorithmically verifying formal systems. This is achieved by verifying whether the model derived from a hardware or software design satisfies a formal specification expressed as a set of logic formulas.

The model of a system is usually expressed as a finite state machine, in other words, a directed graph consisting of vertices and edges. A set of atomic propositions is associated with each vertex, i.e., state. The edges represent possible executions that alter the system's state. Finally, the atomic propositions represent the properties that hold at the given point of execution.

The model checking problem can be stated as follows: given a desired property, expressed as a temporal logic formula  $p$ , and a model  $M$  with initial state  $s$ , decide if the model satisfies the logic formula, or formally

$$M, s \models p$$

#### Model Checking

If model  $M$  is finite, model checking is reduced to a graph search. Unfortunately, this is rarely the case with software systems, and the critical challenge faced by model checking tools is *state explosion*, an exponential growth in the state space. Each model checking technique must address state explosion in order to be able to solve real-world problems.

Researchers have developed several techniques that can help alleviate state explosion, including symbolic algorithms, partial order reduction, binary decision diagrams, and abstraction of uninteresting or non-critical system characteristics. Another strategy for combating the exponential growth in the state space, successfully adopted by Alloy for example [137], is to explicitly bound the size of the state space, thus ensuring the technique's feasibility. Of course, doing so introduces *optimistic inaccuracy* into the analysis process: while no defects may have been found during analysis, there is no guarantee that the model is in fact defect-free.

When using analysis tools such as model checkers, a software system's architects will have to trade-off the risks of undiscovered critical defects against the practical limitations of applying a model checker on a very large architectural model.

### Model-Based Analysis Enabled by ADLs

The types of analyses for which an ADL is well suited depend on its underlying semantic model and, to a lesser extent, its specification features. For example,

- Wright [10] uses communicating sequential processes, or CSP, to analyze a system's connectors and the components attached to them for deadlocks. The objective of the analysis is to identify any conditions under which a component requires access to a currently unavailable system resource in order to continue its processing, but the system is unable to make that resource available. For example, if component  $C_i$  needs to access a record in a database, but that record is locked by another component  $C_j$ , and  $C_j$  is unable to release the lock until some chain of conditions ending with component  $C_i$  is met (e.g.,  $C_i$  may need to free up some other system resource so that  $C_j$  can complete its current task), then the system will deadlock.
- Aesop [86] ensures style-specific topological constraints and type conformance among architectural elements. For example, Aesop will disallow a server to make requests in a client-server architecture.
- MetaH [124] and UniCon [257] support schedulability analysis by specifying non-functional properties, such as the criticality and priority of components. Then techniques such as rate-monotonic analysis [167] are applied to ensure that the architecture as-modeled can in fact accomplish its required functionality. This is particularly important in the case of systems with stringent performance requirements, such as real-time requirements.

Language parsers and compilers are another kind of analysis tools. Parsers analyze architectures for syntactic correctness, while compilers establish semantic correctness. All architecture modeling notations used in practice have parsers. Several—for example, Darwin [176], MetaH, and UniCon—also have compilers of sorts, which enable them to generate executable systems from architectural descriptions, provided that component implementations already exist. Rapide's compiler generates executable simulations of Rapide architectures [170].

Another aspect of analysis is enforcement of constraints. Parsers and compilers enforce constraints implicit in type information, non-functional attributes, component and connector interfaces, and semantic models. Rapide also supports explicit specification of other types of constraints, and provides means for their checking and enforcement. Its Constraint Checker analyzes the conformance of a Rapide simulation to the formal constraints defined in the architecture. An architecture constraint checking tool, Armani [196], which is based on the ACME ADL [90] allows specification and enforcement of arbitrary architectural constraints. UML

allows the specification of architectural constraints in its Object Constraint Language, or OCL, but does not natively enforce those constraints; additional tool support must be obtained or built to do so.

Languages such as SADL and Rapide provide support for refining an architecture across multiple levels of detail. SADL requires manual proofs of the correctness of mappings of constructs between an abstract and a more concrete architectural style. For example, an abstract architectural style can be the dataflow style, a more concrete style would be the pipe-and-filter style, and an even more concrete style would be the pipeline style. The proof in SADL is performed only once; thereafter, SADL provides a tool that automatically checks whether any two architectures described in the two styles adhere to the mapping. Rapide, on the other hand, supports event maps between individual architectures. The maps are compiled by Rapide's Simulator, so that its Constraint Checker can verify that the events generated during simulation of the concrete architecture satisfy the constraints in the abstract architecture.

A summary of the different ADLs' combined analysis foci is given in the table below.

<b>Goals</b>	Consistency Compatibility Completeness (internal)
<b>Scope</b>	Component- and connector-level Subsystem- and system-level Data exchange Different abstraction levels Architecture comparison
<b>Concern</b>	Structural Behavioral Interaction Non-functional
<b>Models</b>	Semi-formal Formal
<b>Type</b>	Static
<b>Automation Level</b>	Partially automated Automated
<b>Stakeholders</b>	Architects Developers Managers Customers

### Reliability Analysis

A software system's reliability is the probability that the system will perform its intended functionality under specified design limits, without failure. A *failure* is the occurrence of an incorrect output as a result of an input value that is received, with respect to the specification. An *error* is a mental mistake made by the designer or programmer. A *fault* or a *defect* is the manifestation of that error in the system. In other words, a defect is an abnormal condition that may cause a reduction in, or loss of, the capability of a component to perform a required function; it is a requirements, design, or implementation flaw or deviation from a desired or intended state.

*Failure* in the above definition denotes that a particular system component is not operational. Reliability can be assessed using several metrics, such as

- *time to failure* – for example, mean time until a system fails after its last restoration,
- *time to repair* – for example, mean time until a system is repaired after its last failure, and
- *time between failures* – for example, mean time between two system failures).

Modeling, estimating, and analyzing software reliability has been an active discipline for several decades. During most of that time, techniques for reliability analysis have been developed and applied at the level of system implementation artifacts. The reason is that several key system parameters are known during or after implementation, including the system's operational profile, and possibly its failure and recovery history. Those parameters are used typically in the creation of a state-based model of the system, in which the probabilities of transitions between the states are derived from the system's operational profile and failure data. Then, this model is fed into a stochastic model such as a Discrete-Time Markov Chain [265], which is solved using standard techniques to determine the reliability of the system in question.

Engineers need not, and should not, wait to estimate the reliability of a system until the system has been implemented, however. A software architectural model can be analyzed for reliability in manner similar to that described above. At the same time, there are several sources of uncertainty inherent in an architectural model that must be addressed:

1. Software developers may work within different development scenarios. Examples development scenarios may include implementing entirely new systems anew, reusing components and/or architectures from previous projects, purchasing software

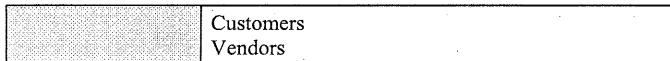
from a vendor, etc. Each scenario introduces different reliability challenges

2. The granularity of the architectural models may vary significantly. A system may be accompanied by coarse-grained models for very large components, partial models for commercial-off-the-shelf components, very detailed models for safety-critical components, etc..
3. Finally, different sources of information about the system's likely usage may be available. Developers may have at their disposal little or no information about an unprecedeted system, a functionally similar system whose usage will also likely be similar, access to experts or extensive domain knowledge, etc.

These types of variation must be accounted for in architecture-level reliability modeling and analysis. As in the case of implemented systems, a state-based model corresponding to the architecture can be constructed. However, certain information such as the operational profile and system failure frequencies cannot be obtained, but must be estimated. For this reason, the reliability values obtained at the level of architecture should not be treated as absolute values, but should instead be qualified by the assumptions, such as the presumed operational profile, made about the system. Furthermore, the uncertainties inherent in the architecture-level reliability model suggest that it may be more meaningful to leverage stochastic models other than DTMCs. One such model, specifically intended to deal with modeling uncertainties, is the Hidden Markov Model, or HMM [233].

The different facets of reliability analysis are summarized in the table below.

Goals	Consistency Compatibility Correctness
Scope	Component- and connector-level Subsystem- and system-level
Concern	Non-functional
Models	Formal
Type	Static Scenario-based
Automation Level	Partially automated
Stakeholders	Architects Managers



### 8.8.3 Simulation-Based Analysis

Simulation requires producing a dynamic, executable model of a given system, or of a part of the system that is of particular interest, possibly from a source model that is otherwise not executable. For example, the model of *QueueServer* component's behavior from Section 8.1, specified in terms of its operations' pre- and post-conditions, is not executable. On the other hand, its interaction protocol from Figure 8-3 can be simulated by selecting a possible sequence of component invocations, which can also be referred to as a sequence of system *events*. This event sequence would be used to execute *QueueServer*'s interaction protocol state machine. For instance, if we assume that the `Empty` state is the start state in the state machine, the following will be valid sequences of events

```
<enqueue, enqueue>
<enqueue, dequeue, enqueue>
<enqueue, enqueue, dequeue, enqueue, dequeue>
```

while the single-event sequence

```
<dequeue>
```

is invalid, as is any sequence that starts with the `dequeue` event or has more `dequeue` than `enqueue` events. Note that the validity of a sequence such as

```
<enqueue, enqueue, enqueue>
```

cannot be established without introducing additional information about the system, namely, the size of the queue.

Simulation need not produce identical results to the system's execution: the source model, such as an architectural model, may elide many details of the system. For example, the *QueueServer* component's model says nothing about the frequency with which the component will be invoked, the sizes of elements that will be placed on the queue, the processing time required to store or access and return the queue elements, and so on. Because of this, the output of simulation might only be observed for event sequences, general trends, or ranges of values rather than specific results. Note that a system's implementation can be thought of as a very faithful executable model. Likewise, running that implementation model can be thought of as a highly precise simulation.

Clearly not all architectural models will be amenable to simulation—recall as a simple example the informal model from Figure 8-1. Even those architectural models that are amenable to simulation may need to be augmented with an external formalism in order to enable their execution. For example, models of event-based architectures may not provide event generation, processing, and response frequencies. To include that information, the architectural model may be mapped, for example, to a discrete event system simulation formalism or a queueing network, with possible ranges of such frequencies specified, and then simulated.

Of course, every time additional information such as event frequency is introduced, architects run the risk of injecting imprecision into the architectural model, and hence into the analysis results. On the other hand, since simulation is tool supported, architects can supply many different values for the model parameters, representing different possible system usage scenarios. They would thereby obtain more precise results than would be possible with “one size fits all” model-based analysis, and do so much more easily and inexpensively than via inspections and reviews.

Several software simulation platforms exist, and different ADLs discussed in Chapter 6 and in the previous section have made use of them. The conceptual relationship between ADLs and simulation models and platforms is depicted in Figure 8-13: certain architectural models (e.g., UML's state-transition-based models or Rapide's partially ordered event-based models) can be simulated directly; other models may require a mapping to the simulation substrate. The required mapping from an architectural model to a simulation model may be partial or complete and of various degrees of complexity, depending on the semantic closeness between the ADL and the simulation platform. In turn, the simulation platform can be executed on top of a specific runtime platform.

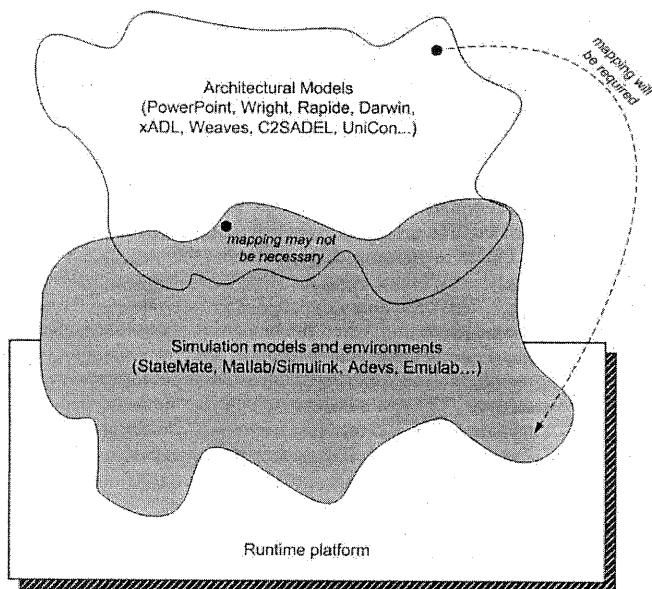


Figure 8-13. The conceptual relationship between architectural and simulation models.

The *goals* of simulation-based architectural analysis techniques can be any of the four “C’s: completeness, consistency, compatibility, and correctness. However, similarly to software testing, because of the nature of simulation these properties can be established only with a limited degree of confidence and possibly only for a particular subsystem or system property.

The *scope* of simulation-based architectural analysis usually is the entire system or a particular subsystem, as well as the dataflow in the system. However, it is possible to isolate individual components and connectors and simulate their behaviors as well. Simulation-based techniques can be particularly effective in assessing the compliance of the given architectural model to a higher-level model from which it has been derived, as well as the model’s similarity to an existing architecture with known properties. Because such models, and thus the results of their simulations, can be expected to differ, additional know-how may be required to determine the exact relationship between the architectural models under consideration.

Since simulation-based analysis techniques allow “running” an architecture and observing the outcome, the *concern* of simulation-based analysis spans behavior, interaction, and non-functional properties. For

example, the architect can target a set of components in the architecture to ensure that they will be able to interact in the desired manner. Again, the degree of architects’ confidence in the analysis results will vary depending on the amount of detail provided in the architectural model. An architect’s confidence in the simulation results will also depend upon his level of confidence that the selected operational scenarios (that is, system inputs) will match the implemented system’s eventual usage. As a very simple example, consider the *QueueServer* component from Figure 8-3: if the architect can be certain that the first invocation of the component in its actual execution environment will never be to dequeue an element, he can trust the results of simulations even if they do not start with a dequeue event.

Simulation-based analysis demands that the architectural *models* be formal. Informal models cannot be mapped to the necessary simulation substrate unless the system’s architects make many impromptu, possibly arbitrary and incorrect, design decisions in the course of the mapping.

The *types* of analysis for which simulation-based techniques are well suited are dynamic and, in particular, scenario-based analysis. Simulation-based techniques are well suited to assessing the system’s runtime behavior, interaction characteristics, and non-functional qualities. If known system usage scenarios are postulated, the architects no longer need to be concerned with the completeness of the analysis results and whether the results will be representative of the system’s actual use.

As already discussed, in terms of *automation level* simulation-based techniques are typically fully automated, requiring no human intervention other than supplying system inputs. However, the process of mapping an architectural model to a simulation model may require significant human involvement. This, in turn, can render the process error prone.

Finally, simulation-driven architecture analysis techniques can be useful to all system *stakeholders*. Setting up and running simulations may require a high degree of technical expertise and familiarity with the architectural model, the architecture modeling notation, as well as the simulation substrate.

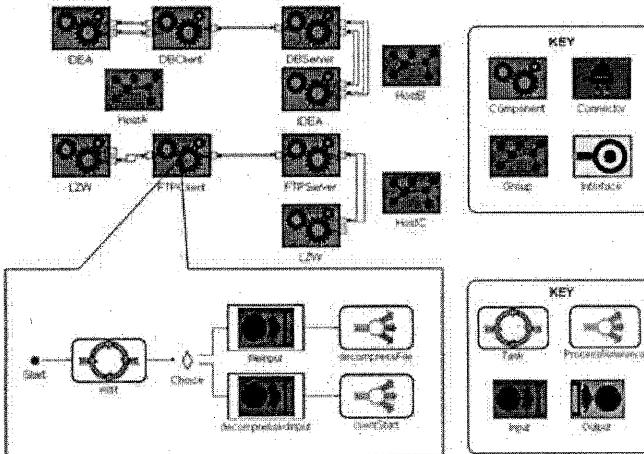
The remainder of this section will discuss a representative example of simulation-driven analysis of architectural models.

## XTEAM

The eXtensible Tool-chain for Evaluation of Architectural Models (XTEAM) is a model-driven architectural description and simulation environment for mobile and resource-constrained software systems [FASE’07]. XTEAM composes two existing, general-purpose ADLs, enhancing them to capture important features of mobile systems. It

implements model generators that take advantage of the ADL extensions to produce simulation models.

For modeling architectural concerns, XTEAM builds an architectural meta-model. This meta-model leverages xADL's Core, which, as the reader will recall from Chapter 6, defines architectural structures and types common to most other ADLs. This meta-model is augmented with finite state processes, or FSP, which allows the specification of component behaviors [177]. The combination of xADL and FSP allows the creation of architectural representations that can be simulated. XTEAM masks many of the details of the two notations via a visual language depicted in Figure 8-14.



**Figure 8-14.** An example XTEAM model of a system comprising three hardware hosts and eight software components. The behavior of one of the components has been highlighted. This behavior represents XTEAM's syntactic overlay on top of FSP. Note that XTEAM allows behaviors to be abstracted in the form of the *ProcessReference* construct.

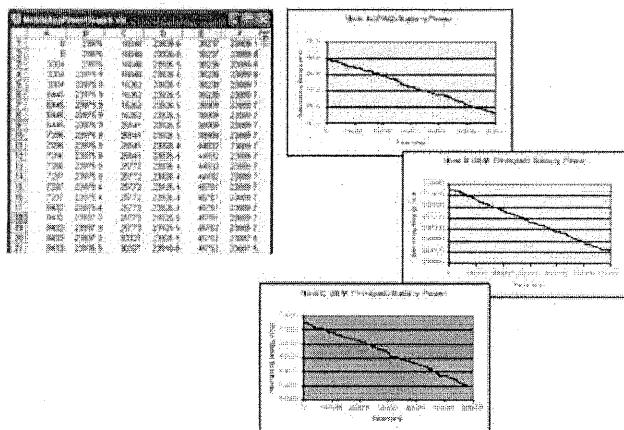
Models conformant to the composed ADL contain sufficient information to implement a semantic mapping into low-level simulation constructs, which can be executed by an off-the-shelf discrete event simulation engine, such as adevs [QRef]. This semantic mapping is implemented by XTEAM's model interpreter framework. When invoked by an architect, the XTEAM interpreter framework traverses the architectural model, building up a discrete event simulation model in the process. The interpreter framework maps components and connectors to discrete event constructs, such as atomic models and static digraphs. The FSP-based behavioral specifications encoded in XTEAM, such as the model shown in the bottom diagram of Figure 8-14, are translated into the state transition

functions employed by the discrete event simulation engine. The interpreter framework also creates discrete event entities that represent various system resources, such as threads. "Hook" methods provided by the framework allow an architect to generate the code needed to realize a wide variety of dynamic analyses.

XTEAM implements simulation-based analysis capabilities for end-to-end latency, memory utilization, component reliability, and energy consumption. Each analysis type requires the implementation of the needed XTEAM ADL extensions and a model interpreter. For example, XTEAM implements the component reliability modeling extension and analysis technique using the HMM-based approach described in Section 8.8.2. This reliability estimation approach relies on the definition of component failure types, the probabilities of those failures at different times during component execution, and the probability of, and time required for, recovery from failure. In order to support this type of analysis, XTEAM's FSP-based behavior language had to be extended to include failure and recovery events and probabilities. XTEAM was then augmented with an analysis technique that determines if and when failures occur as the components in the system progress through different tasks and states.

Another analysis supported by XTEAM is that of the modeled mobile system's energy consumption rate. The selected energy consumption model by Seo [254] was implemented as another XTEAM ADL extension and model interpreter, which incorporated the necessary elements of the energy cost model. Then, another adevs simulation was generated by XTEAM to show the system's likely energy consumption over time, under certain usage assumptions. The results of one such simulation for the architecture depicted in Figure 8-14 is shown in Figure 8-15.

**Figure 8-15.** Energy consumption profile of the architecture from Figure 8-14 obtained from the adevs simulation. The simulation was generated automatically from the XTEAM model.



The below table summarizes XTEAM according to the architectural analysis criteria introduced in this chapter.

Goals	Consistency Compatibility Correctness
Scope	Component- and connector-level Subsystem- and system-level Data exchange
Concern	Structural Behavioral Interaction Non-functional
Models	Formal
Type	Dynamic Scenario-based
Automation Level	Automated
Stakeholders	Architects Developers Managers Customers Vendors

## 8.9 End Matter: Tying It All Together

A major part of what makes good architectural practice is deciding what one wants out of the architecture. An individual or organization cannot and should not focus on architecture just because it is widely accepted that doing so is the right thing to do. Instead, system stakeholders should first decide on the specific benefits they want to gain from the explicit architectural focus. One clear such benefit is the establishment of a system's properties of interest, before the system has been implemented and deployed. Making sure that the system possesses the key required properties, and does not have or is reasonably unlikely to have any undesirable characteristics, is critical. Architectural analysis provides system stakeholders with a powerful suite of techniques and tools for doing that.

However, architectural analysis is not easy. Neither is it cheap (see *The Business Case* sidebar). It should be planned for and applied carefully. The system's stakeholders must be clear about their project objectives, and must then map those objectives to specific architectural analyses. This chapter has provided a structure that can be used to determine which architectural analysis techniques are best suited for which system development scenarios. In many cases, multiple analysis techniques may need to be used in concert. Again, deciding which techniques to use is a critical part of an architect's job: using too many will expend the project's resources unnecessarily; using too few will run the risk of propagating defects into the final system; using wrong analyses will have both of these drawbacks.

### The Business Case

The up-front costs in an architecture-driven software development project can be significant. Even if we consider architectural analysis alone,

1. techniques for architectural inspections and reviews typically involve the participation of many stakeholders over several days — recall ATAM for example;
2. model-based analysis requires the development or acquisition of multiple tools as well as the possible introduction of formalisms, each with its own learning curve, required by those tools — for example, recall the adoption of Markov models for reliability analysis or Wright's incorporation of CSP to ensure deadlock freedom;

3. finally, simulation-based analysis most often requires augmenting the architectural model or recasting it into the form required by the simulation substrate — recall XTEAM’s reliance on xADL, FSP, and adevs.

Clearly, architectural analysis can be costly. These are the very costs of which many managers and organizations are leery since the planned revenue from the system under development is still very far off into the future. Therefore, these costs must be offset by the benefits gained from architectural analysis. The benefits of detecting and removing software system defects early on are well known: many sources, starting with Boehm’s seminal work on *Software Engineering Economics* [ref], have documented that discovering defects earlier rather than later can reduce the cost of mitigating those defects by an order of magnitude or more.

This does not mean that all costs of architectural analysis are automatically justified of course. There is no particular need to do analysis for the sake of demonstrating that one can do it, or in order to show off a technique or tool. Analysis must have a clear objective and take place within a particular, well defined context. Put another way, the undertaken analysis activity must recoup its own costs via the benefits it yields. Nobody should pay more for something than the value it gives them back. For example, a system’s architects should not spend more to perform deadlock analysis than the projected risk and associated cost of deadlock for the system in question. The bottom line for any project with a tight budget—which in practice means, for a great majority of projects—is that under no circumstances should the cost of architectural analysis impinge upon the organization’s ability to actually implement the system.

## 8.10 Review Questions

1. What are the architecture analysis criteria?
2. What are the four “C’s of architectural analysis?
3. What is the difference between internal and external consistency?
4. What is interface inconsistency? Provide an example.
5. What is interaction inconsistency? Provide an example.
6. What are the advantages and disadvantages of informal architectural models as pertaining to analysis?
7. What are the advantages and disadvantages of formal architectural models as pertaining to analysis?
8. Why is system-level analysis important if you have already completed component- and connector-level analysis?

9. Why is the analysis of the data exchanged in an architecture important?
10. Why is it important to analyze an architecture for non-functional concerns?
11. Who are the possible stakeholders in architectural analysis?
12. Is scenario-driven analysis a special case of static analysis or dynamic analysis? Justify your answer.
13. Name some advantages and some disadvantages of architectural inspections and reviews.
14. What is model checking? How does it pertain to architectural analysis?
15. How does one analyze an architecture for deadlocks?
16. What are Discrete Time Markov Chains used for?
17. What is simulation?
18. If an architectural model is expressed in a notation that does not have executable semantics, can it still be simulated? Justify your answer.

## 8.11 Exercises

1. Select one of the models of Lunar Lander from Chapter 4 or Chapter 6. Determine its components. For each individual component, model the services it provides and requires in terms of their names and interfaces. After you have completed the model, analyze the model manually for name and interface inconsistencies.
2. Model the behaviors of the Lunar Lander components used in the previous exercise, by specifying each component operation’s pre- and post-conditions, as discussed in this chapter. After you have completed the model, analyze the model manually for behavioral inconsistencies.
3. As an alternative, or in addition, to the pre- and post-condition based behavior model from the preceding exercise, model the Lunar Lander component behaviors with state-transition diagrams, such as those used by UML. Discuss the specific advantages and difficulties in using this model in ensuring behavioral consistency. Research whether any available techniques can be adopted or adapted for ensuring the consistency of two state-transition diagrams.
4. Select one of the models of Lunar Lander from Chapter 4 or Chapter 6. Determine its components. Construct each component’s interaction model. Analyze these models for interaction inconsistencies. What, if any, are the differences between this task and the task described in the preceding exercise.
5. Download and study the Alloy modeling language and analysis tool suite ([alloy.mit.edu](http://alloy.mit.edu)). Discuss the possible ways in which Alloy can be used to aid architecture modeling and analysis. Demonstrate your arguments with specific examples of simple architectures, architectural properties, architectural styles, and so on.
6. Select an existing application with a documented architecture. This can be an application you have worked on or an open source system. Study the architecture if you are unfamiliar with it. Follow the ATAM

- process to determine the quality attributes important to the system, as well as the architectural decisions employed. Develop a set of scenarios and key decisions underlying the architecture. Use the scenarios to determine whether the architectural decisions result in the required quality attributes.
7. Discuss the potential shortcomings of applying the ATAM process without all the prescribed stakeholders and a separate architecture evaluation team.
  8. Select one of the models of Lunar Lander from Chapter 4 or Chapter 6. Provide its state-based reliability model as discussed in this chapter. Study an existing off-the-shelf technique for reliability estimation (e.g., DTMC or HMM). Apply this technique on your reliability model. Devise strategies for improving your system's reliability.
  9. Select an important property of a software system, such as reliability, availability, or fault-tolerance. State the assumptions required in order to be able to assess this property at the architectural level. Discuss the missing knowledge about the system that necessitates the assumptions. Then discuss the implications and reasonableness of each assumption.
  10. Select two existing ADLs of your choice. Use each ADL to model the Lunar Lander architecture. Use the two ADLs' respective analysis tools to analyze each model for the properties on which the given ADL focuses. Discuss the extent to which the two ADLs' modeling features impact the available analyses versus the extent to which the selected analyses appear to impact the available modeling features.
  11. Download and study an available simulation engine such as adevs (<http://www.ornl.gov/~lqn/adefs/index.html>). Provide a mapping from an ADL of your choice to the simulation engine. Discuss the challenges in doing so and the range of architectural properties for which the simulations can be used. Practically demonstrate the use of simulation for at least one such property.

## 8.12 Further Reading

A significant amount of literature on software architecture has focused on architecture-based analysis. The early work on ADLs, such as Wright and Rapide, focused as much on the enabled analysis techniques as it did on the modeling features. Likewise, when UML first came onto the software development scene in the mid-to-late 1990s as a *de facto* modeling standard, it was almost immediately accompanied by a continuing stream of publications on how UML models can be effectively analyzed for many different types of properties of interest. A widely cited overview of ADLs and their associated analysis capabilities was provided Medvidovic and Taylor in 2000 [189]. That work has been recently revisited and the perspective expanded by Medvidovic, Dashofy, and Taylor [190].

Carnegie Mellon University's Software Engineering Institute has over time proposed a number of architectural analysis approaches that entail

inspections and reviews. Examples are ATAM, studied in this chapter, its precursor software architecture analysis method, or SAAM, and an evaluation method for partial architectures, called ARID. These techniques are described in a book by Clements, Kazman, and Klein [39]. Recently, Dobrica and Niemelä provided a broader survey of inspection and review-based architectural analysis approaches [66].

Leveraging explicit architectural models for determining a system's key non-functional properties has gained a lot of interest over time. This has resulted in a cross-pollination of ideas from established disciplines such as reliability, dependability, and fault-tolerant computing on the one hand, and software architecture on the other hand. In 2007 alone, Immonen and Niemelä [133] have provided a survey of architecture-based methods for availability and reliability estimation, while Gokhale conducted a separate survey of architecture-based reliability analysis approaches [97].

## CHAPTER 9

**9 Implementation**

Implementation is the one phase of software development that is not optional. Regardless of how well the requirements have been captured or how carefully the architecture has been designed and reviewed, software systems must be implemented in code to achieve their ends. Architecture is used to capture important design decisions about a system, using sound engineering principles and knowledge to increase confidence that the target system's qualities match the expectations of its stakeholders. To imbue these qualities in the target system, the implementation must be derived from its architecture.

In terms of implementation, architecture is both prescriptive and restrictive. It is prescriptive in the sense that it gives implementers direction on what to produce—how to structure code modules, how they should be interconnected, and how they should behave. It is restrictive in the sense that its guidelines—particularly those specified in the architectural style—tell developers what they may *not* do: what forms of communication are prohibited, what kinds of behaviors or system states are not allowed, and so on.

The problem of relating architecture to implementation is one of *mapping*. Concepts defined at the architecture level should be directly connected to artifacts at the implementation level. This correspondence is not necessarily one-to-one: in general, a software component or connector will be implemented using many code and resource artifacts. Likewise, a single software library may be shared among several component implementations (as long as its manner of use does not violate style rules). When this mapping is not maintained, architectural degradation can occur—specifically, the gradual deviation of a system's implementation from its architecture. This generally makes software harder to understand and maintain, and makes it difficult to achieve or retain the qualities embodied by the architecture.

Properly implementing an architecture so that it survives in the implementation requires a well-formed understanding of how concepts in the architecture (and the architectural style) map onto target

implementation technologies such as programming languages, development environments, reusable libraries and components, middleware, and component models. These technologies can help, but they can also hinder: they nearly always come with their own assumptions that can influence or get in the way of architectural decisions made earlier. Even concepts we take for granted, such as object-oriented programming languages, can have architectural influences. In this chapter, we will discuss techniques and technologies for creating and maintaining mappings between architecture and implementation.

We will also introduce and focus on a concept known as an *architecture implementation framework*: software that bridges the gap between architectures and implementation technologies. We will discuss how to identify, evaluate, and create new frameworks. We will also relate frameworks to other, similar technologies such as middleware and component frameworks.

## Outline of Chapter 9

9	Implementation
9.1	Concepts
9.1.1	The Mapping Problem
9.1.2	Architecture Implementation Frameworks
9.1.3	Evaluating Frameworks
9.1.4	Middleware, Component Models, and Application Frameworks
9.1.5	Building a New Framework
9.1.6	Concurrency
9.1.7	Generative Technologies
9.1.8	Ensuring Architecture-to-Implementation Consistency
9.2	Existing Frameworks
9.2.1	Frameworks for the Pipe and Filter Architectural Style
9.2.2	Frameworks for the C2 Architectural Style
9.3	Examples
9.3.1	Implementing Lunar Lander in the Pipe-and-Filter Style using the java.io Framework
9.3.2	Implementing Lunar Lander in the C2 Style using the Lightweight C2 Framework
9.4	End Matter
9.5	Review Questions
9.6	Exercises
9.7	Further Reading

**9.1 Concepts**

Here, we will discuss concepts and issues related to architecture-based implementation.

### 9.1.1 The Mapping Problem

As stated above, implementing an architecture is a problem of mapping—specifically, mapping design decisions to specific implementation constructs that realize those decisions. From a software quality perspective, this mapping is known as *traceability*. In general, the term ‘traceability’ can refer to any mechanism for connecting different software artifacts; in this context we specifically mean traceability from architecture to implementation. Choosing how to create and maintain this mapping is critical in architecture-based development. Here, we discuss implementation mappings for the kinds of design decisions discussed in Chapter 6.

**Components and Connectors:** Design decisions about components and connectors partition the application’s functionality into discrete elements of computation and communication. In general, programming environments provide mechanisms such as packages, libraries or classes that are used to partition functionality in implementations. Here, the challenge is to maintain a mapping between the partitions established by the architecture-level components and connectors and the partitions established by the implementation-level packages, libraries, classes, and so on. If implementations are not partitioned according to the component/connector boundaries specified in the architecture, then component boundaries may break down and architectural drift and erosion will occur.

**Interfaces:** At the architecture level, interfaces can be specified in many different ways. If interfaces are specified in terms of method or function signatures similar to those in the target programming language, mapping is a straightforward process of translating the method signatures into code. However, if the architecture-level interface definition is more complex—specifying a protocol or set of state transitions, then greater effort will be required to create an appropriate implementation.

**Configurations:** At the architecture level, configurations are often specified as linked graphs of components and connectors. These graphs specify and constrain how the components and connectors interact through their interfaces. The same interactions and topologies must be preserved in the implementation. Many programming languages include features that allow one module to refer to another module by way of its interface, rather than its implementation (e.g., though explicitly defined interfaces as in Java, or function pointer tables in C). Additionally, some programming languages and middleware systems allow the use of reflection or dynamic discovery to connect and disconnect components at runtime. When these constructs are available, it is often possible for the implementation-level links between components and connectors to be specified independent of

the components/connectors themselves, or even generated from the architecture description.

**Design Rationale:** Design rationale is a construct that often has no specific mapping to implementation, since it is not something that influences the functionality of the application. Often, the best way to retain design rationale during implementation is through comments in the source code or external documentation.

**Dynamic Properties (Behavior):** Depending on how they are modeled, architecture-level behavioral specifications can ease or facilitate implementation. Some behavioral specifications can be directly translated into implementation skeletons or even complete implementations. However, this is not always the case—formal behavioral specifications often lack bindings to programming-language level constructs and therefore it is difficult to determine whether a behavioral specification is actually implemented correctly. Some behavioral specifications are more useful for generating analysis or testing plans rather than implementations.

**Non-Functional Properties:** Implementing non-functional properties is perhaps one of the most difficult propositions in software engineering. The best way to accomplish this is through a combination of techniques—documenting rationale, inspections, testing, user studies, and so on. This difficulty is why refining non-functional properties into functional design decisions (when possible) is so important.

#### One-Way and Round-Trip Mapping

Architectures and implementations must inevitably co-evolve. Architectures can evolve because of changing requirements or increased understanding, and these changes must be propagated to the implementation. Likewise, discoveries and changes made during implementation will affect the architecture. Keeping architecture and implementation in sync is a challenging problem, involving issues of process, tool support, and organizational culture. Aspects of the mapping that lack strong traceability are often the first to diverge.

Maintaining the architecture-implementation mapping in the face of change depends on the process of change. One option is to mandate that all changes begin from the architecture—the architecture is changed first, the mappings to implementation are used, and then the implementation is updated through the use of automated tools or manual processes. This is effectively a one-way mapping. Another option is to allow changes to be initiated in either the architecture or the implementation. In this case, automated tools or manual processes are still used to update the other artifact. This is a two-way mapping.

Two way mappings are better for detecting and resolving architectural drift and erosion, but they are also more complex and expensive to create and maintain. This is sometimes known as a “round tripping” problem because changes have to be mapped from architecture to implementation and back again. The remainder of this chapter will discuss various strategies for maintaining both one-way and round-trip mappings.

### 9.1.2 Architecture Implementation Frameworks

When developing a system, an ideal approach would be to define the architecture and then select implementation technologies (programming languages, software libraries, operating systems, and so on) that most closely match its needs; this limits the difficulty of the mapping problem. This ideal is difficult to achieve—programming languages rarely have explicit support for architecture-level constructs. Moreover, selection of implementation technologies will often be driven by extrinsic or accidental factors such as cost, maturity, platform support, organizational culture, and even wrongheaded requirements specifications or standards.

When the concepts in an architecture don’t match the concepts in your implementation technologies, one good solution is to use (or develop) an architecture implementation framework [180].

**Definition.** An *architecture implementation framework* is a piece of software that acts as a bridge between a particular architectural style and a set of implementation technologies. It provides key elements of the architectural style *in code*, in a way that assists developers in implementing systems that conform to the prescriptions and constraints of the style.

By far, the most common example of an architecture framework in use today is the Standard I/O library in UNIX [294] and similar operating systems. Although you may not recognize it as such, it is actually a bridge between the pipe and filter style, which is character-stream oriented and concurrent, and procedural, nonconcurrent programming languages like C. It provides architectural concepts (e.g., access to interfaces via readable and writable character streams) in a way that fits the target environment (e.g., procedure calls). A fuller discussion of how the Standard I/O library serves as an architectural framework is found later in this chapter.

Architecture frameworks are effectively technologies that assist developers in conforming to a particular architectural style. However, most frameworks will not prevent developers from wandering outside the constraints of the style. For example, just because a UNIX program imports the Standard I/O library does not mean that the program will work in a pipe-and-filter style: it may read and write all its data from named disk files and ignore the standard input and output streams completely.

It is possible to develop applications in almost any architectural style without the use of an architecture framework. However, this usually means weaving the architectural concepts throughout the implementation and makes it difficult to develop and maintain them. In the cases where no framework exists for a particular programming language/operating system combination, developers will usually end up implementing a set of software libraries and tools that amount to an architecture framework anyway.

From an architectural perspective, frameworks are often considered to be a substrate underlying all components and connectors. Therefore, it is unusual to see a framework modeled as a component or connector in the architecture itself. However, frameworks often include implementations for common components and connectors (such as those defined by the style—a pipe connector or an event bus, for example) that serve as implementations for components and connectors that are specified in the architecture.

#### Same Style, Different Frameworks

A single architectural style can be supported by a number of different, alternative frameworks. This can happen for a number of reasons. First, different programming languages and implementation platforms usually require different frameworks. For example, Java applications use classes in the `java.io` package [112] to perform stream input and output; these classes are how Java implements functions similar to the C standard I/O library. C++ programmers can either use the object-oriented `iostream` library or the procedural `stdio` library for the same purpose. Each of these architecture frameworks bridges the same architectural style (pipe and filter) to different implementation technologies (Java, C++, or C).

Sometimes, multiple frameworks for the same style, programming language, and operating system will be developed. Usually, these frameworks distinguish themselves based on different qualities or capabilities. A good example is the “new I/O” (`java.nio`) package in Java [121]: like the older `java.io` package, `java.nio` allows programs to read and write data streams from various sources. However, the `nio` package provides enhanced capabilities such as native support for buffering, better control over synchronization, and the ability to use fast data transfer techniques like memory mapping. Users can choose the appropriate framework for their application based on the quality needs of their applications.

### 9.1.3 Evaluating Frameworks

Frameworks, like any software systems, can vary widely along nearly any quality dimension. This is why many frameworks are often developed to

support the same architectural style in the same environment. Evaluating a framework, then, is similar to evaluating any important software component.

#### **Platform Support**

An architecture framework brings together three key elements: an architectural style, a programming language, and an operating system. One of the most basic criteria for evaluating a framework, then, is basic platform support: once an architectural style has been identified, what architecture frameworks are available for the target programming language/operating system combination? If the project has the freedom to select the implementation platform based on the architecture (which is becoming increasingly rare as software systems are more and more likely to run on existing platforms already in the field) then availability of suitable architecture frameworks should be a criteria for platform selection.

#### **Fidelity**

One quality that is particularly important in architecture implementation frameworks is *fidelity*, specifically fidelity to the target architectural style. To be useful, a framework need not provide direct implementation support for every single design decision in its target style: for example, it may provide communication mechanisms but leave the concurrency of the architecture up to the individual component implementers. Furthermore, frameworks often provide *support* for following stylistic constraints, but not *enforcement*: that is, the framework will make it easy for implementers to follow the constraints of the style, but will not explicitly prevent them from breaking the constraints. More faithful frameworks are generally better at preventing or avoiding architectural drift and erosion. However, this generally comes at a cost: the frameworks are more complicated, bigger, or less efficient.

#### **Matching Assumptions**

Architectural styles induce certain design decisions and constraints on applications. Frameworks can do the same thing—ideally, the decisions and constraints induced by the framework are the same as those induced by the target style. However, styles often leave many aspects of a system unconstrained, and frameworks have the additional responsibility of supporting the concrete implementation activity. For these reasons, frameworks may induce additional constraints on applications. For example, a framework might assume that the system will be instantiated and configured only by the framework, or that individual components and connectors will not start their own threads of control, or that each software component in the architecture can be associated with a module in the target programming language.

Problems can occur when the assumptions of a framework conflict with the assumptions of other implementation technologies used on a project. For example, consider an architecture framework for an object-oriented programming language. This framework might require that every component have a main class that is derived from a base class provided by the framework. However, the project might include several GUI elements, and the GUI toolkit requires that GUI element classes extend base classes provided by the toolkit. If the programming language is one that does not support multiple inheritance (like Java) there is a serious mismatch between the GUI toolkit and the implementation framework. This situation may not even be an architectural mismatch: it is a mismatch of particular implementation decisions. Nonetheless, strategies must be identified to alleviate this situation.

Thus, when evaluating an architecture framework, it is important to enumerate the assumptions it makes about the target application and compare those with the assumptions made by other components, toolkits, libraries, and environments with which the application will interact. Sometimes, workarounds can be developed, especially if the mismatch is a low-level implementation detail. However, if the mismatch is architectural, this might call into question the compatibility of the architectural style itself with the choice of implementation technologies for the implemented application.

#### **Efficiency**

In general, architecture frameworks serve as another layer of functionality between the application and the hardware it runs on. One of the primary dangers of introducing new layers is a decrease in application efficiency. This concern is especially important when dealing with architecture frameworks, since they tend to pervade the application. An architecture framework may mediate all communication between components in a system, for example, or dictate the concurrency policy for the entire application. When this is the case, efficiency should be a primary selection criteria for a framework.

Before committing to a framework, it is a useful exercise to run benchmarks on the framework with parameters derived from the target application to get a feel for the upper bound of application performance using the framework. For example, if a framework can exchange 10,000 messages per minute in a dummy application whose sole purpose is to exchange messages as fast as possible, it is not realistic to build an application that will exchange 20,000 messages per minute along with performing other processing duties.

#### **Other Considerations**

As noted above, the issues involved in selecting an architecture framework are very similar to those involved in selecting any software component. It

could be argued that because frameworks have such a pervasive effect on applications, they are the most critical element of all to choose. Qualities such as size, cost, ease of use, availability of source code, reliability, robustness, portability, and many others are all important when choosing a framework.

#### 9.1.4 Middleware, Component Models, and Application Frameworks

A spectrum of technologies exists to integrate software components and provide services above and beyond those provided by a given programming language/operating system combination. These technologies go by a number of different names: middleware, component models (or component frameworks), and application frameworks. We will refer to these systems collectively as ‘middleware.’ Popular examples include CORBA [209], JavaBeans [143], COM/DCOM/COM+ [255], .NET, Java Message Service [144], and so on.

There are many similarities between architecture frameworks and middleware. Both of them provide developers with implementation services that are not natively available in the underlying programming language or operating system. For example, CORBA middleware provides services such as Remote Procedure Calls (RPCs) and the ability to dynamically discover the interfaces of objects. The JavaBeans component model introduces a new concept to Java: the Bean, an object that follows certain interface guidelines that make it possible to compose Beans more easily.

Architecture implementation frameworks are a form of middleware. The difference between traditional middleware and architecture frameworks is the focus on architectural style. Architecture implementation frameworks are implemented specifically to support development in one or more architectural styles: here, the *style* is the primary artifact driving the implementation technology. Middleware is created based on what *services* are provided, generally without regard to the style of the application being developed.

##### How Middleware and Component Frameworks May Induce a Style

Middleware often constrains applications in ways that are similar to architecture frameworks. Middleware often influences how an application’s functionality is broken up into components, how those components interact (often through middleware-provided services akin to connectors) and also the application’s topology. These are generally architectural concerns. In this sense, middleware can *induce* an architecture or architectural style on an application [61].

CORBA (and CORBA-like technologies such as COM and RMI [104]) are a good example of how middleware can influence application

architectures. CORBA breaks an application up into objects that may reside on different hosts. Objects that participate in the application expose their own services through provided interfaces whose method signatures are specified in an interface definition language (IDL). Objects look up other objects through services such as naming services or trading services, and then call each other using a request-response pattern, passing only serializable parameters across the interface boundaries. Together, these constraints comprise an architectural style that might be referred to as the ‘distributed objects’ style.

If system stakeholders have chosen the distributed objects style for their application, then CORBA-like middleware might serve as an ideal architecture framework. However, things are rarely this simple. Presented with an application to design, software architects have to make hundreds of design decisions. Among the most important decisions they will make are choosing the application’s architectural style. However, experienced architects are also familiar with many different middleware technologies and the advantages of those technologies. The services provided by many middleware technologies can be seductive, and often the capabilities of a particular middleware system will influence an architect’s decision-making process. Architects must be especially careful to avoid having a middleware technology overly influence their designs.

##### Resolving Mismatches between Architectural Styles and Middleware

Two major conflicts can arise between architectural styles and middleware:

1. The architectural style chosen for the application does not match that induced by the middleware chosen.
2. The application’s designers choose a middleware first based on services provided and let this have an undue influence over the architectural style of the application.

When selecting implementation technologies, it is critical to understand that the quality *benefits* provided by that technology often come with architectural implications, which may not be compatible with your architecture’s design. For example, CORBA provides the *benefits* of distribution and reflection, but in a form that induces systems that are based on objects that communicate by request-response procedure calls, which induces certain architectural drawbacks, such as increased latency and synchronization. Allowing the choice of middleware to influence the architecture is backwards: it is the tail wagging the dog. Architecture should influence your choice of middleware.

When there is an architectural mismatch between middleware and the target architectural style, several options are available:

**Change the style:** The architectural style can be changed to better fit the middleware. This should be done only when the benefits of using the middleware outweigh the costs of adapting it to work with the target style.

**Change the middleware:** The middleware can be adapted to better fit the architectural style. This strategy is often difficult because middleware packages are often large, complex, or proprietary.

**Develop glue code:** Architecture frameworks can be built on top of middleware, leveraging the parts of middleware that match, and working around the parts that do not. This way, neither the style nor the middleware itself has to be adapted.

**Ignore unneeded middleware services:** Some middleware packages or component frameworks might provide a host of services that cut across many aspects of application development. However, it may be possible to use a subset of these services selectively, and ignore the services that are not compatible with (or relevant to) the target architectural style.

**Hide the middleware:** Developers use middleware because it provides certain services. If those services are not necessarily cross-cutting, and can be applied at specific points in the architecture, then it may be possible to “hide” the middleware inside individual components or connectors. For example, if CORBA is only being used to facilitate communication between heterogeneous components running on different hosts, all CORBA-related code can be isolated to individual connectors that need cross-host communication. Other CORBA services such as lookup and dynamic interface discovery might be entirely used within the context of the connectors or ignored entirely.

#### Using Middleware to Implement Connectors

As mentioned above, many middleware packages provide services that are effectively communication-centric: they provide different mechanisms for heterogeneous components to communicate. If improving communication in an architecture is a goal, then using middleware as the basis for implementing *connectors*, rather than the whole application, can allow a system to avoid having the middleware’s assumptions bleed into and corrupt the architecture’s design decisions.

In this scenario, architects should define and identify the capabilities required for a connector first, ideally without regard to how that connector will be implemented. Then, middleware should be selected that can provide all (or most) of those capabilities and also fit with the other project goals. If capabilities are *not* provided directly by the middleware, they should be implemented as part of the connector’s implementation. The result is a connector that fulfills the architectural need, rather than one that bows to assumptions made by middleware developers.

For example, a connector might be needed that provides message-passing support between a C++ component running on Linux with a Java component running on Windows. Two message-oriented middleware packages may be available: a commercial package that has C++ and Java support for both platforms, but is proprietary and expensive, and an open-source solution that supports both platforms but only C++ components. If budgets are tight, the open-source solution can be selected, and a Java Native Interface (JNI) adapter [165] can be written to allow the Java component to communicate with the middleware.

#### 9.1.5 Building a New Framework

Occasionally, a situation arises where the most reasonable solution is to develop a new architecture implementation framework. Good reasons to develop a new framework include:

- The architectural style in use is novel;
- The architectural style is not novel but it is being implemented on a platform for which no framework exists; or
- The architectural style is not novel and frameworks exist for the target platform, but the existing frameworks are inadequate.

Developing an architecture framework is a task that should not be approached lightly. These frameworks will impact almost every part of the applications built atop them and can be a make-or-break factor for the success of those applications, so great care should be undertaken in their design. Developing an architecture framework is, in many respects, like developing any other application—it requires the development of requirements, a design, input from many stakeholders, quality evaluation, and so on. As such, almost everything we have said in this book about developing applications in general can be applied to architecture frameworks. There are some additional guidelines that can be applied specifically to framework development, however:

**Have a good understanding of the style first:** Developing an architecture framework with an incomplete understanding of the target architectural style is a recipe for disaster. There will be no standard by which to measure the framework for fidelity or completeness. A clear, concise set of the rules of the architectural style should be developed before framework design begins.

**Limit the framework to issues addressed in the architectural style:** To the greatest extent possible, an architecture implementation framework should be independent from any specific target application. Including application-specific features (that are not part of the style) in a framework

limits the reusability of the framework and blurs the line between what is part of the application and what is part of its style.

**Choose the scope of the framework:** Well-implemented architecture frameworks are valuable reusable assets for the organizations that develop them. Developers of a new framework must decide how the framework will be reused in the future to properly scope its capabilities. For example, a particular architectural style may be amenable to dynamic architectures—those that change their structure on the fly. However, the initial target applications built in the style may not take advantage of this. Whether or not to implement dynamism in the framework depends on how likely it is that dynamism will be needed in a future project (or a future version of the current project). This leads to a related piece of advice:

**Avoid over-engineering:** When building new frameworks, it is tempting to include all sorts of clever or useful capabilities, regardless of whether the target applications will actually use them. This is especially true because frameworks are often (and should be) developed separately from specific applications. These additional capabilities can involve additional layers and levels of abstraction and have significant effects on the framework, particularly on its usability and performance.

**Limit overhead for application developers:** Every framework puts some additional burden on application implementers—to include boilerplate code in components, to implement a standard set of behaviors that the framework can call upon, and so on. As burdens on application developers increase, frameworks become more cumbersome and less palatable. Limiting their additional obligations (either through framework design or tool support) can mitigate this.

**Develop a strategy for legacy and off-the-shelf resources:** Almost any application is bound to include resources (components, connectors, middleware, and so on) that were not developed with the framework in mind. Without a documented or tool-supported strategy for integrating these external resources, developers will be forced to come up with their own mechanisms on an ad-hoc basis. This can cause problems as developers re-invent the wheel (or worse, re-invent different wheels). Framework developers should strongly consider what kinds of external resources might be incorporated in applications and establish strategies for integrating these resources to distribute with the framework.

### 9.1.6 Concurrency

With the advent of fast machines, nimble operating systems, multi-core processors, and ubiquitous networks of independent hosts, it is rare that any system be designed without some aspect of concurrency: multiple tasks in the system occurring simultaneously [177]. Concurrency is

generally implemented with a variety of strategies: on a single host, multiple threads or operating system processes are generally employed. On a network, different hosts necessarily run independent processes that must work together and negotiate the behavior of the system as a whole.

Most architectural styles have some notion of concurrency, whether it is simple synchronization or complex multi-processing. Pipe-and-filter, one of the simplest styles, was developed to take advantage of concurrency to process partial results in a way that batch processing systems were unable to. Many of the architectural styles identified in Chapter 4 have specific provisions for which elements can (or should) run concurrently.

Many architecture implementation frameworks and middleware packages have concurrency management as one of their primary features. Later in this chapter, two example implementations of Lunar Lander in both the pipe-and-filter and C2 architectural styles are presented. In both cases, concurrency is handled entirely by the underlying framework or operating system: in the case of the pipe-and-filter system, each filter runs in a concurrent process; in the case of the C2 system, each component and connector runs in its own thread of control.

Ideally, primary concurrency decisions will be made at the architectural level. If this is the case, most concurrency can be handled directly in the architecture framework. Because concurrency bugs can lead to race conditions and deadlock—two of the most difficult faults to reproduce and track down—getting concurrency ‘right’ in an architecture is critical. Encapsulating the implementation of concurrency in well-tested framework or middleware code can help to mitigate the risks of deadlock and race conditions (although it cannot eliminate them).

### 9.1.7 Generative Technologies

One proposed “silver bullet” that has received quite a bit of attention over the years is the idea that software system implementations can be made much more efficient and effective by generating (parts of) those implementations directly from their designs. Indeed, this is the focus of the OMG’s Model Driven Architecture initiative [199], described in Chapter 16, as well as many generative technologies that have been developed over the years.

Because generation can derive (partial) implementations directly from designs, generation is an attractive strategy for maintaining the mapping from architecture to code. However, it is generally not a comprehensive (or easy) solution to implement properly. Some generative strategies that can be employed in architecture-centric development are described here:

**Generation of complete implementations of systems or elements:**

Given a detailed enough architectural specification, including structural, interface, and complete behavioral specifications, it is possible to generate a complete implementation for a component, connector, or even an entire system. When this strategy is employed, architectural drift and erosion can be (at least partially) eliminated, since implementations are simply transformations of the architecture. In practice, however, this is extremely difficult, due to the extensive amount of detail needed to generate implementations—the behavioral specifications for a component, for example, are usually of equal complexity to code implementing the component.

**Generation of skeletons or interfaces:** It is also possible to generate partial implementations of elements or systems from architectural models. For example, if interfaces are well-described, it is possible to generate code skeletons for each service or method in the interface, and allow implementers to fill in the behavior. Likewise, if partial behavioral specifications are available (in the form of statecharts, for example), a finite-state automata can be generated in code with the behavior for each state left up to coders.

**Generation of compositions:** In situations where a library of reusable component and connector implementations is already available and systems are simply composed from this library, architectural models can be used to generate the configurations and “glue code” needed to connect the elements into a complete system. This strategy is generally most effective in the context of domain-specific software engineering (see Chapter 15).

In any generative effort, the round-tripping problem becomes paramount. In the context of generation, one-way approaches allow one artifact to be generated from another—for example, for code to be generated from architectural models. Round-trip approaches allow changes in the target artifact to be reflected back in the source artifact automatically. For example, in a one-way approach, a component in an architectural model might result in the creation of a new Java package containing class files. In a round-trip approach, the creation of a new Java package might result in the generation of a new component in the architectural model, as well. In general, this requires maintaining some metadata in the generated code—usually in specially formatted comments. While round trip approaches are preferable to one-way approaches, they are generally tricky to implement correctly, especially when architectural modeling and code development tools are not well-integrated (as is often the case).

**9.1.8 Ensuring Architecture-to-Implementation Consistency**

Even with the use of an architectural framework, it is rarely obvious whether an implementation actually conforms to its prescribed architecture. Determining whether this is the case will generally require a combination of techniques, including manual inspection and review. There are several strategies that can make this task easier.

**Create and maintain traceability links from architectural elements to implementation elements:** The existence of links, or explicit mappings, from architectural elements to implementation elements can assist developers in determining whether each architectural element has a corresponding implementation and vice-versa. Having these links makes it easier to determine whether something has been inadvertently ignored. If these links are to concrete parts of an architecture model and/or concrete implementation artifacts, then automated link checking can be used to determine whether any links have broken due to changes in either the model or the implementation. This strategy works well for concrete artifacts, but mapping across different levels of abstraction or elements that do not have a direct architecture-to-implementation transition can be tricky.

**Make the architectural model part of the implementation:** An architectural model may contain information that can be used directly in a system’s implementation. For example, a description of a system’s structure in a model (indicating how components are to be instantiated and connected) can be used as an implementation artifact. A tool can be used to extract information about components, connectors, and their topology directly from the architecture description and wire the system up in this way automatically. This can be done at build time or during system startup. In either case, one form of architecture-implementation correspondence is guaranteed, because the structure of the implemented application is derived directly from the architectural model.

**Generate some or all of the implementation from the architecture:** Depending on the form and contents of an architectural model, it may be possible to generate portions of an implementation directly from the model using automated tools. If the set of components in a system is specified and the architectural style of the application is known, it is possible to generate component skeletons for target architecture implementation framework. If behavioral information is also available in the model, it may be possible to generate some or all of the implementations of those components from the model.

## 9.2 Existing Frameworks

This section will survey a sample of architecture implementation frameworks that have been implemented for various architectural styles, show how they satisfy our definition of a framework, and evaluate their strengths and weaknesses.

### 9.2.1 Frameworks for the Pipe and Filter Architectural Style

Earlier in the chapter, we noted that many programmers have used an architecture framework without necessarily being aware of it—an architecture framework for the pipe-and-filter style. Nearly every programming language implemented on every major operating system is bundled with a library or module that serves as an architecture framework for the pipe-and-filter style.

#### The Standard I/O Framework

The C programming language is single-threaded, uses call-return control flow for procedures and functions, and generally stores and retrieves all data from memory by address. How, then, is the C language made compatible with the pipe-and-filter style, where filters can run in parallel, are generally activated when data becomes available, and filters retrieve and send data through byte streams? The answer is in an architecture framework provided in the form of the standard input-output (I/O) library, also known by its abbreviated name, ‘`stdio`’.

Recall that an architecture framework serves as a bridge between the needs of an architectural style and the services provided by the programming language and the operating system. Here, the programming language provides few services: without libraries like `stdio`, the C programming language does very little at all. The operating system, however, is quite complicit in this situation: the underlying operating system provides concurrency at the process level<sup>9</sup> as well as at least two distinguished data streams to each filter process (“standard input” and “standard output”).

<sup>9</sup> When implementations of C are available on an operating system that supports process concurrency such as UNIX or Windows, the operating system process scheduler will generally be used to assign CPU time to each filter. However, pipe-and-filter has also been supported on single-process operating systems like DOS: in this case, the filters were run entirely in sequence and the output of each filter was stored in a temporary file on the hard disk until the next process could start to process it. This effectively turned all pipe-and-filter applications into batch-sequential applications when run in DOS.

The `stdio` library provides C programs access to the operating system’s provided standard input/output streams through a procedural API that treat the streams in the same way as files on a sequential-access storage device. Low-level routines such as `getchar(...)` and `putchar(...)` allow programs to read and write a single byte at a time; more complex routines such as `scanf(...)` and `printf(...)` allow the reading and writing of larger quantities of formatted data. Depending on how streams are implemented in the underlying operating system, different `stdio` implementations may employ techniques such as buffering to improve performance. Different implementations may also have different abilities with respect to blocking: if bytes are written to an output stream, and the next filter in the pipeline is not ready to consume those bytes, then `stdio` may cause the write operation to block (make the caller wait) until the receiver is ready, or it may buffer the data and allow the caller to continue.

This is certainly not the only way that such a framework could be implemented. For example, one could imagine a framework where bytes arriving on the standard input triggered the program to begin execution, rather than the operating system invoking the program’s `main(...)` method.

With this understanding, we can now evaluate the `stdio` framework in terms of the qualities we laid out earlier.

**Platform support:** The `stdio` interface is standardized, and its implementation ships with every implementation of the C programming language, but is relatively specific to that language. Similar libraries may exist in other languages. Implementations of the framework on platforms with little or no operating system support for streams as an interprocess communication mechanism may be more complicated, or may not support pipe-and-filter applications at all.

**Fidelity:** The `stdio` library’s support for streams is good, but a program that uses it is not constrained to working as a filter. Programs are free to ignore both the standard input and output streams, and do input/output through other mechanisms (interfacing directly with the keyboard or using GUI libraries for data output).

**Matching Assumptions:** The default assumptions of the `stdio` library with respect to pipe-and-filter systems is that each filter will be a separate operating system process and the operating-system-provided streams (standard input and standard output) will be used for communication. If the application wants to use pipe-and-filter differently (e.g., with filters as portions of a C application running in a single process, or perhaps using a disk file as intermediate storage), then the application has to be modified somewhat. Because the `stdio` library provides practically identical

interfaces for reading and writing to different kinds of streams (file streams, in-memory streams, interprocess streams and so on) this widens the kinds of pipe-and-filter applications that can be built with it.

**Efficiency:** Whether filters run concurrently (one of the key efficiency benefits of pipe-and-filter over batch-sequential architectures) is largely dependent on how the underlying operating system schedules processes. For single-process operating systems, output has to be stored in shared memory or secondary storage as each filter runs sequentially. Largely, the `stdio` library itself has no control over how this is handled.

#### The `java.io` Framework

The Java programming language is multi-threaded, object-oriented, uses call-return method calls for transfer of control and bundles code and data within objects. The object classes that are used for constructing pipe-and-filter applications in Java are found in the package `java.io`. Although these classes share a purpose with C's `stdio` library, their design is different. The `java.io` class library defines two primary base classes: `InputStream`, which allows callers to read a sequence of bytes, and `OutputStream`, which allows callers to write a sequence of bytes. Each of these provides minimal sets of methods, for reading and writing single bytes or groups of bytes, as well as a few auxiliary methods for 'rewinding' within a stream during reading, or flushing writes.

These low-level base classes define minimal functionality for readable and writable byte streams. These classes are not used directly; instead, derived classes provide concrete functionality. In `java.io`, two kinds of derived classes are provided. One set of derived classes provide sources and sinks for the data bytes: files, network sockets, in-memory byte arrays, and so on. In addition, three distinguished objects are provided by the runtime environment: `System.in`, `System.out`, and `System.err`, which are used for reading from and writing to the standard input, output, and error streams of the process and are used for creating multi-process pipe-and-filter applications. Another set of derived classes adds functionality to the basic input and output streams by wrapping these low-level streams. For example, `BufferedInputStream` and `BufferedOutputStream` wrap other streams, but add buffers to improve performance when reading or writing large amounts of bytes at once. `DataInputStream` and `DataOutputStream` add additional interface methods to wrapped streams that allow the reading and writing of basic Java data types (integers, floats, and so on).

With this in mind, we can now evaluate `java.io` and contrast it with the `stdio` library.

With this understanding, we can now evaluate the `stdio` framework in terms of the qualities we laid out earlier.

**Platform support:** The `java.io` library is part of the standard set of Java packages, and so is available on any platform that can run Java. Platform-specific features such as file naming conventions and locating the standard input and output streams are abstracted away (to the degree possible) by the class library.

**Fidelity:** The library's support for streams is comprehensive, but as with `stdio`, programs that use this library do not have to work as a filter. On the other hand, pipe-and-filter architectures running within a single program are easier to construct with `java.io` due to the existence of streams that read from and write to memory, and in-process pipe classes that allow in-process streams to be connected.

**Matching Assumptions:** The `java.io` library matches the assumptions of the pipe-and-filter style well. In-process pipe-and-filter structures can be constructed with relative ease due to Java's innate support for threading, and the ability to run multiple internal filters concurrently. Programmers must be careful, however, to avoid deadlock—default operations in `java.io` are blocking, and programmers must explicitly ask whether bytes are available in a stream before reading them if they want to implement non-blocking behavior instead.

**Efficiency:** Java gives programmers fine-grained control over efficiency mechanisms—buffers can be used by wrapping a stream in a buffered stream; threads can be explicitly allocated to separate I/O operations from computationally intensive operations (which can increase performance on multi-processor machines). However, with increased cooperation from the operating system, it is often possible to achieve even higher efficiency. This motivated the construction of the later `java.nio` (New I/O) package, which can take advantage of faster mechanisms.

#### 9.2.2 Frameworks for the C2 Architectural Style

Constructing applications in the C2 architectural style [276] (see Chapter 4) differs markedly from traditional procedure-call and object-oriented programming. It imposes strict rules on how applications are constructed internally and how components within an application communicate. It governs both transfers of control and data within an application, and makes assumptions about concurrency and threading. Because of these differences, frameworks are essential for effective C2 development.

Challenges addressed by a C2 framework arise from the various C2 architectural style constraints. For example, C2 requires that application functionality be partitioned into discrete components (for computation)

and connectors (for communication). A framework must provide support, at the programming-language level, for application developers to partition their functionality into modules. C2 components and connectors communicate via asynchronous messages, and should operate as if they run in separate threads of control. Frameworks supporting this constraint must provide a concept of an asynchronous message, and must allocate (from the operating system) or simulate (via a technique such as round-robin scheduling of a single thread's activities) multiple threads of control within the application's components and connectors.

C2 frameworks have been developed for many platform/language combinations. C2 Frameworks have been developed for C++, Ada, Java, and other languages running on Windows, UNIX, the Java Virtual Machine, and so on. Several different Java C2 frameworks have been developed, each with different characteristics. We will compare and contrast two of these frameworks: a basic framework called the Lightweight C2 Framework, and a later, larger—but more configurable—framework called the Flexible C2 Framework.

#### The Lightweight C2 Framework

The first C2 framework implemented in Java is known as the Lightweight C2 framework, implemented in only 16 classes (about 3000 lines) of Java code.

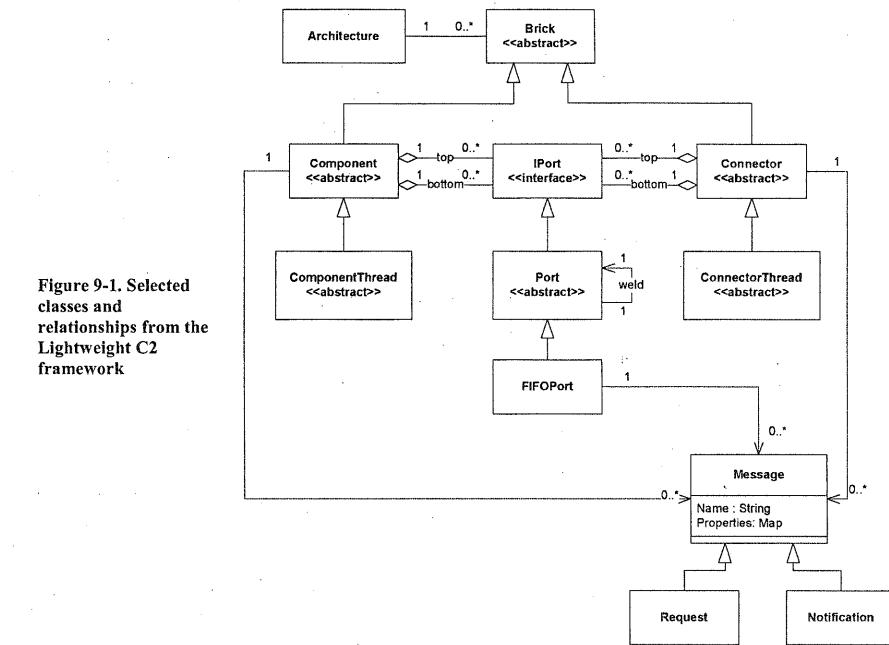


Figure 9-1. Selected classes and relationships from the Lightweight C2 framework

Figure 9-1 shows a selected set of classes from the Lightweight C2 Framework, as well as their relationships, as a UML class diagram. To implement an application using this framework, developers create component and connector implementations as subclasses of the **Component** or **Connector** abstract base classes. Developers may create additional classes as needed that are called by these component and connector classes, as well. The component and connector classes communicate with each other using only messages, which are instances of the **Request** and **Notification** classes. The developer then creates a main program that uses the interface of the **Architecture** class to instantiate and hook up the various components and connectors.

The diagram shows some of the key design choices made by the framework authors. C2 components and connectors are implemented as Java classes that extend abstract base classes (**Component** and **Connector**) provided by the framework. Messages are encoded as

objects with a string name and a String-to-Object property map, containing the message contents.

Certain aspects of the framework—such as threading and message queuing—are left up to individual components and connectors. Two threading policies are available to implementers: if application developers extend the base classes Component and Connector, a single application thread will service the entire application. Developers using this strategy must be careful that they do not block this thread and inadvertently hang their applications. If developers extend the base classes ComponentThread and ConnectorThread, then each component or connector gets an independent thread of control. This takes up more resources, but also reduces the possibility of inadvertent deadlock. Message queuing is handled through Port objects, which are objects that are capable of receiving incoming messages for a component or connector. Note that ports are a concept introduced entirely by this framework—they are not part of the C2 style itself. The framework provides only one kind of port: a first-in-first-out (FIFO) queue. With FIFO ports, messages are processed in the order received—no message is given priority over any other. Developers are free to implement their own non-FIFO ports as long as those ports extend the abstract Port class.

It is also interesting to note that not every constraint of the C2 style is reflected in the framework. For example, nothing in the framework enforces the rule that components and connectors must act as if they run in separate memory spaces. In a single-process application, if a component or connector inserts a Java object reference into a message object, other components or connectors could modify this object directly without sending any messages. This would constitute illegal communication in the C2 style. However, Java does not have any support for the concept of separate in-process memory spaces, so enforcing this constraint in a framework would be prohibitively expensive. This represents a situation in which fidelity is traded for efficiency, and where a framework is used to aid, but not enforce, implementations that conform to the target style.

### The Flexible C2 Framework

This framework was developed later, and incorporates more aspects of the architectural style directly into the framework. As such, it is larger—73 classes (approximately 8500 lines of code).

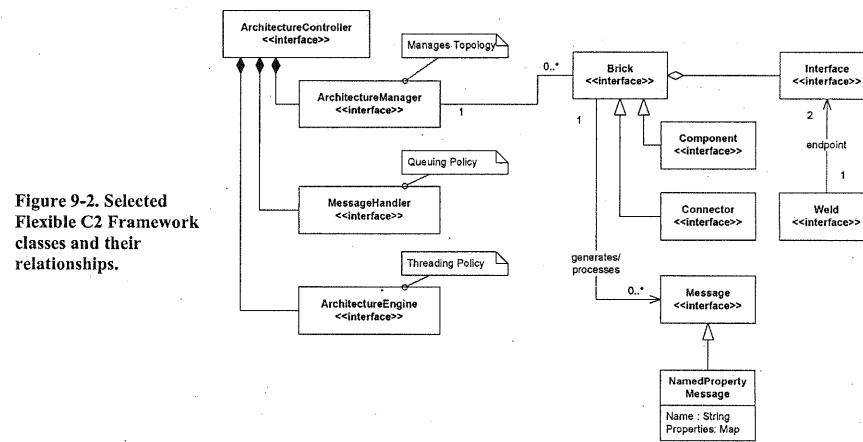


Figure 9-2. Selected Flexible C2 Framework classes and their relationships.

Figure 9-2 shows a similar set of selected classes in the Flexible C2 framework. Application developers using this framework follow a similar course of action to those using the Lightweight C2 framework. They first implement application components and connectors as classes that implement the Component and Connector interfaces. These classes exchange data through objects that implement the Message interface. They then write a main class that instantiates, connects, and starts these components and connectors using the ArchitectureController interface.

One obvious difference between the two frameworks is the Flexible C2 Framework's pervasive use of Java interfaces to represent fundamental concepts rather than abstract base classes. As a programming language, Java allows only single inheritance among object classes. However, a single class can implement multiple interfaces. The use of Java interfaces rather than abstract base classes makes the Flexible C2 Framework somewhat easier to adapt to different contexts than the Lightweight C2 Framework. Components, connectors, and messages created by developers can extend any other base class as long as they implement the appropriate interface. Some boilerplate code is required to implement each interface, and so the framework provides abstract base classes (not shown in Figure 9-2) for each interface for the common situation in which developer classes are not required to extend an external base class.

Another obvious difference is in the implementation of the application threading and message queuing policies. In the Lightweight C2

Framework, these policies were distributed throughout the application in individual components, connectors, and ports. In the Flexible C2 Framework, these concerns are centralized through classes called *MessageHandlers*, which define queuing policies, and *ArchitectureEngines*, which define threading policies. This allows developers to define and select these policies on an application-wide basis.

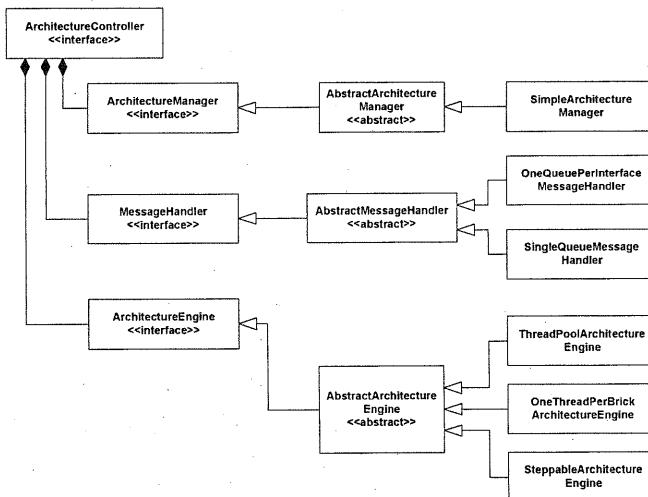


Figure 9-3. The implementation of pluggable message queuing and threading policies in the Flexible C2 Framework.

Figure 9-3 shows how queuing and threading policies can be ‘plugged in’ to an application. The interfaces, *MessageHandler* and *ArchitectureEngine*, define internal APIs common to all queuing and threading policies. *AbstractMessageHandler* and *AbstractArchitectureEngine* abstract base classes implement boilerplate functions common to all queuing and threading policies. Finally, the framework provides several alternative concrete queuing and threading policies that can be selected for an application. Available queuing policies include:

**One-Queue-Per-Interface:** Each interface (in the C2 style, ‘top’ or ‘bottom’ interfaces) gets its own message queue.

**One-Queue-Per-Application:** All messages for the application are stored in a single queue.

Available threading policies include:

**One-Thread-Per-Brick:** Each brick (component or connector) in the architecture gets its own thread of control for processing its messages.

**Thread Pool:** The application gets a pool of threads that are shared among all components. When a brick has a message waiting, a thread is dispatched to the brick to process the message. When the message processing completes, the thread returns to the pool.

**Steppable Engine:** A special case of the thread pool policy, the application gets one thread that is controlled by a GUI. When the user presses a ‘step’ button, the thread is dispatched to process a single message. In this way, applications can be more easily debugged.

All of these policies are allowable within the C2 style, but dramatically affect how applications are developed and how much component developers have to consider when writing code. For example, it would be relatively difficult to change a Lightweight C2 Framework application from a one-thread-per-brick to a stoppable threading policy, since this would require changes to each component and connector’s code. In the Flexible C2 framework, this change can be done in one line of code in the application’s main class. On the other hand, centralized, uniform policies can make it more difficult to implement applications in which different individual components and connectors need different local behavior with respect to queuing and threading.

Both C2 frameworks address similar subsets of the C2-style constraints—for example, neither explicitly addresses the requirement that components and connectors are not allowed to communicate through shared memory. As explained above, this requirement is simply too expensive to implement in Java.

#### Comparing the Lightweight and Flexible C2 Frameworks

Because both C2 frameworks address the same architectural style and the same platform, they can be compared directly along numerous dimensions. The first is the technical dimension—examining how each framework supports (or does not support) each of the constraints of the C2 architectural style:

C2 Style Constraint	Lightweight Framework support	Flexible Framework support
Application functionality must be partitioned into	Abstract base classes are extended by application	Interfaces define the requirements for

components and connectors.	developers to create components or connectors; all application functionality must be implemented within or called by these extended base classes.	components and connectors; boilerplate code is provided in abstract base classes that implement these interfaces. All application functionality must be implemented within or called by these extended base classes.
All components and connectors communicate through two interfaces, ‘top’ and ‘bottom.’	Abstract base class provides methods sendRequest() and sendNotification() for emitting top/bottom messages, respectively, and handleRequest() and handleNotification() for receiving top/bottom messages.	Base class provides a sendToAll() method that takes interface (top or bottom) as a parameter, and handle() method that is called when a message is received on any interface. Messages are tagged with the interface they arrived on.
Components and connectors should operate as if they run in their own threads of control.	Threads are created by component and connector base classes.	Threads are controlled by a central threading policy object called an ArchitectureEngine. Different engines can provide alternative threading policies.
Messages sent to the top interface of a component or connector should be received on the attached component/connector bottom(s), and vice-versa.	Methods sendRequest() and sendNotification() look up connected components and connectors and directly enqueue messages in queues belonging to those elements.	Message queuing policy is centralized in an object called a MessageHandler. MessageHandlers ensure that messages get deposited in appropriate queues for processing.
Components and connectors should operate as though they do not share memory; all messages exchanged must be serializable.	Message objects are structured as sets of name-value pair properties, where both names and values are strings.	All messages must implement the java.io.Serializable interface, but are not constrained to any particular format. An implementation of name-value pair set messages is

		also provided.
Components may be connected to at most one connector on each side; connectors may be connected to zero or more components or connectors on each side.	Connecting a component to more than one connector on any side will result in the previous connection being undone before the new one is created.	No explicit support; developers are assumed to check this constraint.
Components may make assumptions about services provided above, but no assumptions about services provided below.	No explicit support; developers are assumed to build components in a way that obeys this constraint.	No explicit support; developers are assumed to build components in a way that obeys this constraint.

Another way of comparing the frameworks is to use the rubric we established earlier:

Concern	Lightweight Framework	Flexible Framework
<i>Platform support</i>	Java Virtual Machine on multiple platforms	Java Virtual Machine on multiple platforms
<i>Fidelity</i>	Assists developers in dealing with many C2-style constraints but does not actively enforce them.	Assists developers in dealing with many C2-style constraints but does not actively enforce them.
<i>Matching Assumptions</i>	Component and connector main classes must inherit from provided abstract base classes; all communication must be through messages that consist of string names and name-value pair properties.	Component and connector main classes must implement from provided Java interfaces; all communication must be through messages which can be in any serializable format.
<i>Efficiency</i>	Framework is small and lightweight; can use only a single thread of control if desired but this risks application deadlock.	Framework is larger but more flexible; can select from many queuing and threading policies to tune efficiency on an application-by-application

	basis.
--	--------

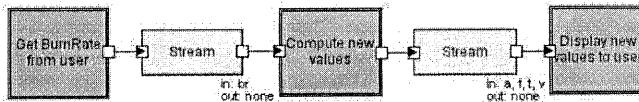
## 9.3 Examples

Throughout the book, we have introduced many architectural design alternatives for the Lunar Lander application. Chapter 4 presents a catalog of architectural styles, with the Lunar Lander designed to fit the constraints of each style. Here, we will examine how architecture frameworks that we have introduced earlier in the chapter can be used to assist in the construction of working Lunar Lander implementations in two of those styles: pipe-and-filter and C2.

Note that the following sections will include code samples showing actual implementations of Lunar Lander. Here, certain good coding practices, such as the use of externalized string constants, comprehensive exception and null-value checking, and so on will be left out for simplicity's sake. Real implementations should take these practices into account as they apply equally when doing architecture-based software development.

### 9.3.1 Implementing Lunar Lander in the Pipe-and-Filter Style using the java.io Framework

Figure 9-4. Lunar Lander in the pipe-and-filter architectural style.



Recall the introduction of a pipe-and-filter-style Lunar Lander architecture from Chapter 4, as shown in Figure 9-4. Here, Lunar Lander is broken up into three components: the first gets the burn rate from the user, the second computes new values, and the third outputs those values back to the user. Communication among the components is one-way and is done through character streams as mandated by the style.

Assuming we want to implement this application in Java, we have two obvious choices for architecture frameworks: the `java.io` package and the `java.nio` package. Because the amount of data being transferred is small and we want a simple implementation, we will implement the system using `java.io`. The next choice we must make is whether to implement the system as an in-process or multi-process system:

**In-Process:** In an in-process system, each component will be implemented by one or more Java classes. These will communicate by way of internal

streams, leveraging internal stream classes provided by the `java.io` framework. The application configuration will need to be created in an application `main` method that we write.

**Multi-Process:** In a multi-process system, each component will be implemented by one or more Java classes comprising a small application. They will communicate by way of the operating-system-provided streams `System.in` and `System.out`, and the operating system will also provide the pipe connectors. The application configuration will be done on the command-line.

For simplicity, we will implement the application as a multi-process system: this saves us from having to write additional code creating our own pipes and doing tasks such as data buffering and threading—the operating system's internal services will provide buffers among the filters as well as process-level concurrency.

The first task in implementing the Lunar Lander application is to implement the three filters depicted in the proposed architecture. Because the filters are independently composable, this can be done in any order, although the order of implementation does have practical consequences. For example, in a large application, you may want to implement stubs and skeletons for testing purposes, and whether you implement the application from left-to-right or right-to-left has implications on what sorts of stubs and skeletons you must implement. For our application, we will implement from left-to-right, starting from the 'GetBurnRate' filter.

Recall that, in a pipe-and-filter application, all data travels from left-to-right in character streams. If applications need to communicate structured data, that structure must be encoded in the character streams. Additionally, in a strict pipe-and-filter application, all user input comes from the system input stream on the leftmost filter, and all output to the user console comes from the system output stream on the rightmost filter.

In this application, we will need to send structured data down the pipeline. We will use a simple encoding scheme: messages will be separated by newline characters, and each message will be preceded by a control character indicating the type of message. We will preface user-output messages with a pound-sign ('#') and data messages with a percent-sign ('%'). There is nothing particularly special about these characters; they are chosen arbitrarily for this example.

Figure 9-5. The GetBurnRate filter for Lunar Lander.

```
//Import the java.io framework
import java.io.*;

public class GetBurnRate{
```

```

public static void main(String[] args){
    //Send welcome message
    System.out.println("#Welcome to Lunar Lander");

    try{
        //Begin reading from System input
        BufferedReader inputReader =
            new BufferedReader(new
                InputStreamReader(System.in));

        //Set initial burn rate to 0
        int burnRate = 0;
        do{
            //Prompt user
            System.out.println(
                "#Enter burn rate or <0 to quit:");

            //Read user response
            try{
                String burnRateString = inputReader.readLine();
                burnRate = Integer.parseInt(burnRateString);

                //Send user-supplied burn rate to next filter
                System.out.println("%" + burnRate);
            }
            catch(NumberFormatException nfe){
                System.out.println("#Invalid burn rate.");
            }
        }while(burnRate >= 0);
        inputReader.close();
    }
    catch(IOException ioe){
        ioe.printStackTrace();
    }
}
}

```

Figure 9-5 shows the ‘GetBurnRate’ filter implementation for Lunar Lander. This component effectively represents the user interface of the application. First, it opens a BufferedReader on the system-provided class System.in, which the Java virtual machine connects to the operating system’s input stream. BufferedReader is a class provided by the java.io package for reading structured data such as lines and integers from a character stream. Next, it enters a loop, continually prompting the user for a new burn rate, reading the value, and sending it on to the next filter.

Figure 9-6. The CalcNewValues filter for Lunar Lander.

```

import java.io.*;
public class CalcNewValues{

```

```

public static void main(String[] args){
    //Initialize values
    final int GRAVITY = 2;
    int altitude = 1000;
    int fuel = 500;
    int velocity = 70;
    int time = 0;

    try{
        BufferedReader inputReader = new
            BufferedReader(new InputStreamReader(System.in));

        //Print initial values
        System.out.println("%a" + altitude);
        System.out.println("%f" + fuel);
        System.out.println("%v" + velocity);
        System.out.println("%t" + time);

        String inputLine = null;
        do{
            inputLine = inputReader.readLine();
            if((inputLine != null) &&
                (inputLine.length() > 0)){
                if(inputLine.startsWith("#")){
                    //This is a status line of text, and
                    //should be passed down the pipeline
                    System.out.println(inputLine);
                }
                else if(inputLine.startsWith("%")){
                    //This is an input burn rate
                    try{
                        int burnRate =
                            Integer.parseInt(inputLine.substring(1));
                        if(altitude <= 0){
                            System.out.println("#The game is over.");
                        }
                        else if(burnRate > fuel){
                            System.out.println("#Sorry, you don't" +
                                "have that much fuel.");
                        }
                        else{
                            //Calculate new application state
                            time = time + 1;
                            altitude = altitude - velocity;
                            velocity = ((velocity + GRAVITY) * 10 -
                                burnRate * 2) / 10;
                            fuel = fuel - burnRate;
                            if(altitude <= 0){
                                altitude = 0;
                                if(velocity <= 5){
                                    System.out.println("#You have" +
                                        "landed safely.");
                                }
                                else{

```

```
        System.out.println("#You have" +
                           "crashed.");
    }
}
//Print new values
System.out.println("%a" + altitude);
System.out.println("%f" + fuel);
System.out.println("%v" + velocity);
System.out.println("%t" + time);
}
catch(NumberFormatException nfe){
}
}
}
}while((inputLine != null) && (altitude > 0));
inputReader.close();
}
catch(IOException ioe){
    ioe.printStackTrace();
}
}
```

Figure 9-6 shows the implementation of the ‘CalcNewValues’ filter for Lunar Lander. This is the most complex of the three filters—it must read the new burn rate from the ‘GetBurnRate’ filter, store and update the application’s state, and then send output values to the final filter, which formats those values for display. The basic structure of the filter is similar to that of ‘GetBurnRate’—the program opens a reader on the system input stream, processes the input, and writes data to the system output stream. Here, the filter reads two kinds of data from GetBurnRate: user messages and burn rates. User messages are passed unchanged to the next filter; burn rates trigger a computation. When a new burn rate is read, the filter updates its internal state values—the current altitude, velocity, fuel, and time—and sends those new values to the next filter. It continues until the altitude reaches zero (or less), at which point it determines whether the Lander crashed or landed successfully—either way, the game is over.

The same control character scheme is used in this filter: user messages are prefaced with pound signs and data messages are prefaced with percent signs. The data messages are further coded with a second character indicating the type of data: altitude, fuel, velocity, or time. As should be obvious by this point, ensuring that the various filters have matching assumptions about the encoding scheme is critical in constructing a working application. The encoding scheme is, in effect, the interface contract for the pipe-and-filter application.

Figure 9-7. The DisplayValues filter for Lunar Lander.

```

import java.io.*;
public class DisplayValues{
    public static void main(String[] args){
        try{
            BufferedReader inputReader = new
                BufferedReader(new InputStreamReader(System.in));
            String inputLine = null;
            do{
                inputLine = inputReader.readLine();
                if((inputLine != null) &&
                    (inputLine.length() > 0)){
                    if(inputLine.startsWith("#")){
                        //This is a status line of text, and
                        //should be passed down the pipeline with
                        //the pound-sign stripped off
                        System.out.println(inputLine.substring(1));
                    }
                    else if(inputLine.startsWith("%")){
                        //This is a value to display
                        if(inputLine.length() > 1){
                            try{
                                char valueType = inputLine.charAt(1);
                                int value =
                                    Integer.parseInt(inputLine.substring(2));
                                switch(valueType){
                                    case 'a':
                                        System.out.println("Altitude: " +
                                            value);
                                    break;
                                    case 'f':
                                        System.out.println("Fuel remaining: " +
                                            value);
                                    break;
                                    case 'v':
                                        System.out.println("Current Velocity: " +
                                            value);
                                    break;
                                    case 't':
                                        System.out.println("Time elapsed: " +
                                            value);
                                    break;
                                }
                            }
                            catch(NumberFormatException nfe){
                            }
                        }
                    }
                }
            }while(inputLine != null);
            inputReader.close();
        }
    }
}

```

```

        }
        catch(IOException ioe){
            ioe.printStackTrace();
        }
    }
}

```

Figure 9-7 shows the implementation of the ‘DisplayValues’ filter for Lunar Lander. The structural similarities to the other two filters are again evident here—the filter reads lines from system input and writes them to system output. The purpose of this filter is simply to format data for output to the console. Unformatted user messages from previous filters are output directly, while data values are annotated with descriptions for output. Here, control characters are parsed on input, but no control characters are written to the output stream—the application assumes that it is the final filter in the application and that the output data is intended for display on a console rather than as input to another application filter.

Together, these three filters make up the Lunar Lander application. One task remains, which is to determine how to instantiate and connect the application. This is done easily on the command-line:

```
java GetBurnRate | java CalcNewValues | java DisplayValues
```

This command-line invokes all three filters as separate processes. (The need for the invocation of ‘java’ in each process is an artifact of how the Java Virtual Machine works: each process is an instance of the virtual machine running the class passed as the first parameter to the ‘java’ command). Input from the console is fed to the system input stream of the leftmost filter (GetBurnRate). The output of GetBurnRate is piped to the input of CalcNewValues. The output of CalcNewValues is likewise piped to the input of DisplayValues, and output to the console comes from the system output stream of that filter.

#### Reflections on the Pipe-and-Filter Lunar Lander Implementation

The architecture framework (java.io) in this implementation of Lunar Lander provides several useful services to the application. It includes a number of classes for reading and writing to the system input and output streams (such as BufferedReader). These classes allow data to be read from and written to character streams such as the system input and output streams in different ways: as individual characters, lines, integers, and so on. This allows the implementation to focus more on application functionality and less on the constraints of the architectural style.

The operating system itself provides the pipe connectors, as well as the concurrency policy for the architecture. The filter implementations in this system are closely aligned with the properties of the underlying

framework and operating system, although this is not necessarily obvious from reading the code. For example, the filters assume that they are going to be running concurrently. In some operating systems, such as MS-DOS, pipe-and-filter applications actually run in batch mode, collecting all the output from each filter before sending it to the next filter. If this version of Lunar Lander were to operate in batch mode, user messages sent out by the first two filters would not be output by the third filter until all the input to the first filter was completed. The application would not work properly in this circumstance. Additionally, the filters assume that lines written to the system output stream will be flushed to the next filter automatically. If this were not true, output messages would appear late and the application would operate in a broken or confusing way. These potential mismatching assumptions are subtle, but critical to determining whether an application will operate as desired or not.

The implementation activity is often the time where underspecified or deficient architectures become evident. For example, the (admittedly simple) architecture for pipe-and-filter Lunar Lander specifies what data should pass from filter to filter, but not the format of that data. A component that communicated using XML-based data encoding, while being compatible with the architecture, would not interoperate with the filter components implemented above. Clearly, this architecture has not been elaborated to a point where component interoperability can be inferred from the architecture alone. A mismatch between XML and line-oriented data formats would be easily caught during system integration, but more subtle bugs can be even more dangerous. For example, in the case of the Mars Climate Orbiter, an interface mismatch between metric and Imperial units of measure was a substantial cause for the loss of the orbiter.

#### 9.3.2 Implementing Lunar Lander in the C2 Style using the Lightweight C2 Framework

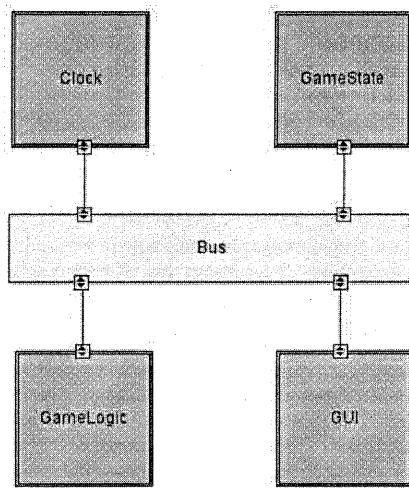


Figure 9-8. Lunar Lander in the C2 architectural style.

Now consider a C2-style Lunar Lander architecture, as shown in Figure 9-8. This version of Lunar Lander is somewhat different from the pipe-and-filter version. First, the application functionality is broken up differently. Here, a game state component retains all game state and broadcasts updates to other components. A game logic component reads the game state, calculates a new state, and updates the game state component with that state. The GUI component is responsible for reading new burn rate values from the user and keeping the user informed as to the current game state. The most significant departure from the pipe-and-filter version is the addition of a clock component, which emits ‘tick’ events, or messages, at periodic intervals. This changes the character of the game substantially: instead of waiting indefinitely for a new burn rate value from the user as in the pipe-and-filter version, this version of Lunar Lander is played in real-time. In this version, the game state changes whenever the clock ticks, and not when new burn rate values are entered. Here, the user may update the current burn rate as often as desired between ticks. When the clock ticks, the current burn rate value is used to calculate the new game state.

As discussed earlier, many C2 frameworks exist for different programming languages and platforms. Assuming we want to implement the system in Java, we still must choose between frameworks such as the Lightweight C2 Framework and the Flexible C2 Framework. Because it results in slightly simpler component code, we will use the Lightweight C2 framework for this implementation.

As with the pipe-and-filter example, we can implement these components in any order, but the order we choose has practical consequences. Because of the substrate independence (i.e., layering) rules in C2, lower components may make assumptions about the services provided by upper components, and vice-versa. (Note that this is reversed from traditional layered or virtual-machine depictions where upper layers are dependent on lower layers). This means that the topmost components have no dependencies, and that lower components are progressively more dependent. We will take a least-dependent-first implementation strategy, which means that the topmost components get implemented first.

```

import c2.framework.*;
public class GameState extends ComponentThread{
    public GameState(){
        super.create("gameState", FIFOPort.class);
    }
    //Internal game state and initial values
    int altitude = 1000;
    int fuel = 500;
    int velocity = 70;
    int time = 0;
    int burnRate = 0;
    boolean landedSafely = false;
    protected void handle(Request r){
        if(r.name().equals("updateGameState")){
            //Update the internal game state
            if(r.hasParameter("altitude")){
                this.altitude =
                    ((Integer)r.getParameter("altitude")).intValue();
            }
            if(r.hasParameter("fuel")){
                this.fuel =
                    ((Integer)r.getParameter("fuel")).intValue();
            }
            if(r.hasParameter("velocity")){
                this.velocity =
                    ((Integer)r.getParameter("velocity")).intValue();
            }
            if(r.hasParameter("time")){
                this.time =
                    ((Integer)r.getParameter("time")).intValue();
            }
            if(r.hasParameter("burnRate")){
                this.burnRate =
                    ((Integer)r.getParameter("burnRate")).intValue();
            }
            if(r.hasParameter("landedSafely")){

```

Figure 9-9. The GameState component in C2.

```

        this.landedSafely =
            ((Boolean)r.getParameter("landedSafely"))
                .booleanValue();
    }

    //Send out the updated game state
    Notification n = createStateNotification();
    send(n);
}

else if(r.name().equals("getGameState")){
    //If a component requests the game state
    //without updating it, send out the state

    Notification n = createStateNotification();
    send(n);
}

protected Notification createStateNotification(){
    //Create a new notification comprising the
    //current game state

    Notification n = new Notification("gameState");
    n.addParameter("altitude", altitude);
    n.addParameter("fuel", fuel);
    n.addParameter("velocity", velocity);
    n.addParameter("time", time);
    n.addParameter("burnRate", burnRate);
    n.addParameter("landedSafely", landedSafely);
    return n;
}

protected void handle(Notification n){
    //This component does not handle notifications
}
}

```

The code for the GameState component is shown in Figure 9-9. The first line of code imports the ‘c2.framework’ namespace, which belongs to the Lightweight C2 framework. The class declaration shows that the GameState class extends the ComponentThread base class. This base class is extended by all component classes that run in their own thread of control (as is the norm in C2-style systems). This base class provides the code required for the component to receive and send requests and notifications, as well as the threading and synchronization code required to coordinate with the other components and connectors.

The first method, GameState(), is a simple boilerplate constructor. This C2 framework requires that each component and connector be given a name (in this case, ‘gameState’), as well as the class that will implement the ports (i.e., message queues) used to exchange messages with attached

connectors. For simplicity, all components and connectors in this architecture will use FIFO (first-in, first-out) ports—that is, ordinary queues.

The next block of code declares a set of member variables that represent the game state—velocity, altitude, fuel remaining, current burn rate, whether the Lander has landed safely, and so on. These will be read and updated as the game is played.

Each component and connector in the Lightweight C2 framework has two primary responsibilities: handling requests (messages traveling upward in the architecture and arriving on the bottom port) and handling notifications (messages traveling downward in the architecture and arriving on the top port).

The next method, handleRequest(), is called automatically by the framework when a request arrives for this component. Recall that in the Lightweight C2 Framework, all requests and notifications have the same structure: a character string name, plus a set of name-value pair properties. This method handles two requests: an updateGameState request and a getGameState request. Upon receiving an updateGameState request, the component reads from the property set various new state values corresponding to elements of the game state. After updating the game state with the new values, the component always creates and emits a new gameState notification containing all the updated state values. Upon receiving a getGameState request, the component simply creates a new game state notification with current state values and sends it out. Sending out a request or a notification in the Lightweight C2 framework is simple—first, a new Request or Notification object is created, given a name, and populated with properties. This object can be passed to a send() method present in the abstract base class—in this case, ComponentThread. The framework routes the message appropriately.

The handleNotification() method for this component is empty; this component does not handle notifications. Because we are aware, from an architectural perspective, that no components will be connected above this one, then we know that it will not receive any.

Effectively, this component is entirely reactive. It spends its time idle until a request arrives on its bottom port. If the request is of a recognized type (updateGameState or getGameState), then the component reacts, either updating its internal state and sending out a new state notification, or simply sending out the current game state. This is a relatively typical pattern of interaction for state components in C2-style systems. It is also worth noting that this component acts entirely as a data structure—data validation and processing is done in other components (primarily the

GameLogic component). Maintaining this separation allows architects to more easily swap out different data structures or game logic components.

```
import c2.framework.*;
public class Clock extends ComponentThread{
    public Clock(){
        super.create("clock", FIFOPort.class);
    }
    public void start(){
        super.start();
        Thread clockThread = new Thread(){
            public void run(){
                //Repeat while the application runs
                while(true){
                    //Wait for five seconds
                    try{
                        Thread.sleep(5000);
                    } catch(InterruptedException ie){}
                    //Send out a tick notification
                    Notification n = new Notification("clockTick");
                    send(n);
                }
            };
            clockThread.start();
        }
        protected void handle(Notification n){
            //This component does not handle notifications
        }
        protected void handle(Request r){
            //This component does not handle requests
        }
    }
}
```

The code for the Clock component is shown in Figure 9-10. The basic scaffolding for this component is similar to that for the GameState component—this component also extends ComponentThread and includes the same boilerplate constructor. Unlike the GameState component, however, the Clock handles neither requests nor notifications. Its job is simply to emit tick notifications at a pre-defined interval. This is done through the creation of a new clock thread in the component's start() method. The start() menu is another distinguished method in the Lightweight C2 Framework; it is called by the framework automatically when the application starts. In this implementation, the

Figure 9-10. The Clock component in C2.

clock thread creates and emits a new tick notification every 5 seconds (5000 milliseconds). The use of a separate clock thread is needed because the component's internal thread (provided by the ComponentThread base class) is used only for handling notifications and requests—attempting to co-opt it for sending out ticks may interfere with the message handling behavior of the component.

```
import c2.framework.*;
public class GameLogic extends ComponentThread{
    public GameLogic(){
        super.create("gameLogic", FIFOPort.class);
    }
    //Game constants
    final int GRAVITY = 2;
    //Internal state values for computation
    int altitude = 0;
    int fuel = 0;
    int velocity = 0;
    int time = 0;
    int burnRate = 0;
    public void start(){
        super.start();
        Request r = new Request("getGameState");
        send(r);
    }
    protected void handle(Notification n){
        if(n.name().equals("gameState")){
            if(n.hasParameter("altitude")){
                this.altitude =
                    ((Integer)n.getParameter("altitude")).intValue();
            }
            if(n.hasParameter("fuel")){
                this.fuel =
                    ((Integer)n.getParameter("fuel")).intValue();
            }
            if(n.hasParameter("velocity")){
                this.velocity =
                    ((Integer)n.getParameter("velocity")).intValue();
            }
            if(n.hasParameter("time")){
                this.time =
                    ((Integer)n.getParameter("time")).intValue();
            }
            if(n.hasParameter("burnRate")){
                this.burnRate =
                    ((Integer)n.getParameter("burnRate")).intValue();
            }
        }
    }
}
```

Figure 9-11. The GameLogic component in C2.

```

else if(n.name().equals("clockTick")){
    //Calculate new lander state values
    int actualBurnRate = burnRate;
    if(actualBurnRate > fuel){
        //Ensure we don't burn more fuel than we have
        actualBurnRate = fuel;
    }

    time = time + 1;
    altitude = altitude - velocity;
    velocity = ((velocity + GRAVITY) * 10 -
        actualBurnRate * 2) / 10;
    fuel = fuel - actualBurnRate;

    //Determine if we landed (safely)
    boolean landedSafely = false;
    if(altitude <= 0){
        altitude = 0;
        if(velocity <= 5){
            landedSafely = true;
        }
    }

    Request r = new Request("updateGameState");
    r.addParameter("time", time);
    r.addParameter("altitude", altitude);
    r.addParameter("velocity", velocity);
    r.addParameter("fuel", fuel);
    r.addParameter("landedSafely", landedSafely);
    send(r);
}

protected void handle(Request r){
    //This component does not handle requests
}
}

```

The code for the GameLogic component is shown in Figure 9-11. This component is the most complex of the C2 Lunar Lander components. Structurally, it is very similar to the GameState component. Instead of responding to requests from lower components, however, it reacts to notifications coming from upper components. GameLogic responds to two kinds of notifications. The first is a gameState notification from the GameState component. Whenever the GameLogic component is notified that the game's state has changed, it updates internal state that is used for later calculation. For a simple game like Lunar Lander, where nearly all the game state is used by the single GameLogic component, keeping separate copies of the game state in the GameState and GameLogic components may seem redundant. In more complex applications, however, logic components rarely need all the game state—instead, they would retain only the parts of the state necessary to do their own computations.

An additional question that might occur to developers familiar with procedural or object-oriented programming is why the GameLogic component does not simply query the GameState component for data when it is needed. The answer lies in the architectural style—in C2, such synchronous component-to-component queries are not allowed.

The second notification handled by the GameLogic component is a clock tick from the Clock component. Recall that this version of Lunar Lander is driven not by user input of new burn rates, but by the tick of the real-time clock. When a clock tick occurs, the latest game state stored in the GameLogic component is used to calculate the next state—burning some amount of fuel, descending (or ascending) a certain distance, and so on. This state is then sent to the GameState component in an updateGameState request, which we saw handled by that component, above.

One additional detail in the GameLogic implementation is the start() method. On startup, the GameLogic component sends an asynchronous request upward to the GameState component for the initial game state. Without doing so, the calculation that occurs on the first clock tick might be based on incorrect (i.e., all-zero) values as initialized in the GameLogic component.

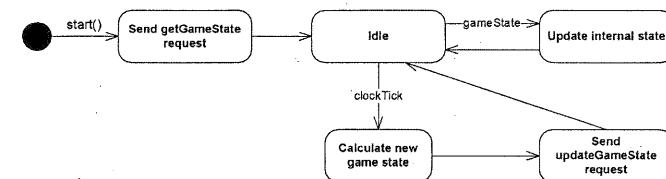


Figure 9-12. Statechart describing the behavior of the GameLogic component in C2.

Effectively, the behavior of the GameLogic component can be summed up by the statechart in Figure 9-12. The component starts and sends a getGameState request upward. It then idles, waiting for notifications. When a gameState notification is received, the internal state of the component is updated. When a clockTick notification is received, a new game state is calculated and a request to update the game state is sent upward.

Figure 9-13. The GUI component in C2.

```

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import c2.framework.*;

```

```

public class GUI extends ComponentThread{
    public GUI(){
        super.create("gui", FIFOPort.class);
    }

    public void start(){
        super.start();
        Thread t = new Thread(){
            public void run(){
                processInput();
            }
        };
        t.start();
    }

    public void processInput(){
        System.out.println("Welcome to Lunar Lander");
        try{
            BufferedReader inputReader = new BufferedReader(
                new InputStreamReader(System.in));

            int burnRate = 0;
            do{
                System.out.println("Enter burn rate or <0" +
                    " to quit:");
                try{
                    String burnRateString = inputReader.readLine();
                    burnRate = Integer.parseInt(burnRateString);

                    Request r = new Request("updateGameState");
                    r.addParameter("burnRate", burnRate);
                    send(r);
                }
                catch(NumberFormatException nfe){
                    System.out.println("Invalid burn rate.");
                }
            }while(burnRate >= 0);
            inputReader.close();
        }
        catch(IOException ioe){
            ioe.printStackTrace();
        }
    }

    protected void handle(Notification n){
        if(n.name().equals("gameState")){
            System.out.println();
            System.out.println("New game state:");

            if(n.hasParameter("altitude")){
                System.out.println(" Altitude: " +
                    n.getParameter("altitude"));
            }
            if(n.hasParameter("fuel")){

```

```

                System.out.println(" Fuel: " +
                    n.getParameter("fuel"));
            }
            if(n.hasParameter("velocity")){
                System.out.println(" Velocity: " +
                    n.getParameter("velocity"));
            }
            if(n.hasParameter("time")){
                System.out.println(" Time: " +
                    n.getParameter("time"));
            }
            if(n.hasParameter("burnRate")){
                System.out.println(" Current burn rate: " +
                    n.getParameter("burnRate"));
            }

            if(n.hasParameter("altitude")){
                int altitude =
                    ((Integer)n.getParameter("altitude")).intValue();
                if(altitude <= 0){
                    boolean landedSafely =
                        ((Boolean)n.getParameter("landedSafely"))
                            .booleanValue();
                    if(landedSafely){
                        System.out.println("You have landed safely.");
                    }
                    else{
                        System.out.println("You have crashed.");
                    }
                    System.exit(0);
                }
            }
        }
    }

    protected void handle(Request r){
        //This component does not handle requests
    }
}

```

The code for the GUI component of the Lunar Lander is shown in Figure 9-13. This component handles all interaction with the user. This particular implementation uses simple console (i.e., text)-based input and output routines. The GUI component has two primary responsibilities. First, it creates an independent thread for reading user input—in this case, burn rates—from the console. Whenever a new burn rate is read, it is wrapped in an updateGameState request and sent upward. Again, a separate thread is needed here to avoid interference with the message processing thread that belongs to the component. Second, the GUI component listens for gameState notifications. Upon receiving an updated game state, the component formats and writes the state to the console.

```

import c2.framework.*;
public class LunarLander{

    public static void main(String[] args){
        //Create the Lunar Lander architecture
        Architecture lunarLander = new
            SimpleArchitecture("LunarLander");

        //Create the components
        Component clock = new Clock();
        Component gameState = new GameState();
        Component gameLogic = new GameLogic();
        Component gui = new GUI();

        //Create the connectors
        Connector bus = new ConnectorThread("bus");

        //Add the components and connectors to the architecture
        lunarLander.addComponent(clock);
        lunarLander.addComponent(gameState);
        lunarLander.addComponent(gameLogic);
        lunarLander.addComponent(gui);

        lunarLander.addConnector(bus);

        //Create the welds (links) between components and
        //connectors
        lunarLander.weld(clock, bus);
        lunarLander.weld(gameState, bus);
        lunarLander.weld(bus, gameLogic);
        lunarLander.weld(bus, gui);

        //Start the application
        lunarLander.start();
    }
}

```

Figure 9-14. The Lunar Lander main program in C2.

Now that all the components have been coded, they must be instantiated and connected together. This is done by way of a main, or bootstrapping program. In the pipe-and-filter example, we were able to use the command-line shell to instantiate and connect the components. For a C2 application, we must instead write this bootstrapping program ourselves, calling upon the services of the Lightweight C2 Framework to instantiate and connect the components. The bootstrapper itself is relatively straightforward. First, an `Architecture` is created, the C2 framework's object that represents an architectural structure. Then, instances of each of the components are created, along with a single connector called `bus`. The components and connectors are added to the `Architecture`, and then links among them (called `Welds` in C2 parlance) are created. With everything connected, the `Architecture`'s `start()` method is called,

which creates internal threads, calls each component and connector's individual `start()` method, and performs other tasks needed to start the application.

## 9.4 End Matter

It is imperative that, to the extent possible, the design decisions in the architecture are reflected in the implemented system. Conflicts or mismatches are the hallmarks of architectural drift and erosion. Sometimes these divergences are obvious and known to the system's stakeholders, and additional documentation of these cases can help to mitigate the risks or provide plans for future work to bring the architecture and implementation back in sync. Sometimes, however, they are not, and stakeholders remain unaware of the problem. This is usually compounded in system maintenance phases, when it is expedient to update the implementation without going back and updating architectural models to match. In some ways, it is more harmful to have conflicting information in the architecture and the implementation than to have an underspecified architecture, since at least an underspecified architecture will not mislead stakeholders.

Maintaining a consistent architecture-to-implementation mapping is almost never easy, and various techniques can be used to do so. The strongest mappings are possible when architectural models become *part of* the system implementation, and are closely connected to implementation artifacts by way of explicit mappings embedded in the models to elements implemented in architecture implementation frameworks. This strategy works well for concrete design decisions, such as structural design decisions, but is more difficult for more abstract design decisions concerning, for example, non-functional properties. In this case, stakeholders must negotiate and make decisions about how they will convince themselves that their architecture is reflected adequately in their implementation. Doubtlessly, this will involve a combined spectrum of strategies from peer review to traceability links between documents to the use of architecture implementation frameworks.

### The Business Case

In general, a good design should result in a good system. The way to maximize your chances of getting a good system out of a good design is to use careful practices for mapping your architecture to your code. A small investment in a good, reusable architecture framework can instill consistency throughout a project and over its lifetime.

Generation technologies are especially powerful in reducing costs and minimizing architectural drift and erosion. While it may not be a silver bullet, generating even partial implementations from architecture is

always vastly superior to making the connection manually, especially if round-trip software engineering is in place. Every line of code written by a *program* rather than a *programmer* is money in the bank.

Maintenance costs are the highest in any successful software engineering project (over 50%). These costs are exacerbated by spaghetti-code, post-hoc changes that (often unknowingly) violate design principles set out at the beginning of the project, and lack of clear understanding of the system. When design principles are violated, the software qualities anticipated and imbued by the design may not manifest themselves in the final, implemented system.

Good architecture-to-implementation mappings help to mitigate risks, especially those due to personnel turnover. Turnover is inevitable in any development effort, and a well-defined architecture with a corresponding implementation will dramatically improve the ability of new personnel to be effective on an old project.

## 9.5 Review Questions

1. What are some architectural concerns that can be mapped to implemented systems? What strategies can be used to map these concerns?
2. What is the difference between one-way and round-trip mapping?
3. What is an architecture implementation framework? How does an architecture implementation framework differ from middleware?
4. What is the relationship between an architecture implementation framework and an architectural style?
5. When might multiple frameworks be developed for a single architectural style?
6. What are some criteria that can be used to evaluate architecture implementation frameworks?
7. How do middleware and component frameworks induce architectural styles?
8. What are some strategies for resolving mismatches between architectural styles and middleware?
9. When should a new architecture implementation framework be developed? What criteria or strategies should be used in developing the new framework?
10. What kinds of generative approaches can assist in moving from architecture to implementation?
11. Enumerate some existing architecture implementation frameworks.

12. How is the standard I/O package an architecture framework for pipe-and-filter systems? How does it support the various rules and constraints of the pipe-and-filter style?

## 9.6 Exercises

1. Run the implemented Lunar Lander applications in this chapter through a debugger and examine how control and data are exchanged through the framework.
2. The chapter compares and contrasts the Lightweight and Flexible C2 Frameworks in terms of both structure and how they support the rules of the C2 style. Perform the same comparison for the java.io and java.nio packages vis-à-vis the pipe-and-filter style.
3. Choose an architecture implementation framework and a simple application, and implement that application atop the framework. Reflect on how you maintained the constraints of the architectural style in your implementation, and how the framework assisted (or hindered) you in doing so.
4. Choose one of the simple architectural styles in Chapter 4 and construct an architecture implementation framework for your preferred platform/operating system combination. Enumerate the rules of the style and how your framework does or does not support those rules.
5. Construct an architecture framework as suggested in Exercise 2, and then use your framework for Exercise 1.
6. Learn about one or more middleware technologies, such as CORBA, COM, RMI, JavaBeans, and so on. Identify the architectural style rules imposed by the middleware platform. Find an example application built atop the middleware and see whether or not it obeys the style rules.

## 9.7 Further Reading

This chapter looks toward architecture implementation frameworks as a primary method of mapping architectural design decisions to implementation artifacts. Surprisingly little has been written on the subject of such frameworks characterized in this way; Malek et. al. [180] is a notable exception. However, many software systems exist that closely resemble architecture implementation frameworks without the explicit focus on styles. Some of these, such as the standard I/O framework in C [151] and the Java I/O [112] and New I/O [121] packages are architecture implementation frameworks in disguise, providing the services of a framework without explicitly being identified as such.

Middleware such as CORBA [209], COM and its variants [255], JavaBeans [143], Java RMI [104], Java Message Service implementations [144] and other message-passing systems like MQSeries [129] and MSMQ [125] are often used as architecture implementation frameworks.

However, Di Nitto and Rosenblum [61] insightfully called out the fact that middleware *induces* an architectural style on applications that use it.

A recent trend, growing in popularity is the extensive use of generative techniques, particularly under the banner of Model-Driven Architecture [199], which can generate whole or partial implementations through models. Generative approaches have been identified as silver bullets before, and time will tell whether MDA lives up to its initial promise.

## CHAPTER 10

# 10 Deployment and Mobility

After a software system has been designed, implemented, and validated, it is ready for operation. That usually requires that the system's components and connectors first be distributed to the "target" hardware processors. A software system cannot fulfill its purpose until it is deployed, that is, until its executable modules are physically placed on the hardware devices on which they are supposed to run. The outcome of the activity of placing a system's software components on its hardware hosts is the *deployment* of the system's architecture.

Once the system is in operation, it is possible, and often necessary, to change the physical location of its hardware hosts. For example, laptop computers, personal digital assistants (PDAs), cellular telephones, software controlled radios, and computers embedded in a vehicle, all move regularly while staying connected. More challenging, more interesting to a software engineer (and even a user), and more pertinent to this book is the relocation or migration of a *software* component or connector from one hardware host to another. This may need to be done to improve the system's performance, perhaps by collocating a processing component with the data it needs, lessen the computational load on a given host, or to achieve some other property. Relocating software modules in this manner changes the deployment view of the software system's architecture during the system's runtime, and is referred to as *migration* or *redeployment*. Runtime system migration (or redeployment) is thus a type of a software system's *mobility*.

It should be noted that changing a system's deployment while it is running in many ways entails a superset of concerns engineers face during initial deployment:

- During a component's migration, its runtime state may need to be preserved and migrated. On the other hand, during initial deployment, prior to system start-up, components are typically stateless.

- Systems experience temporary downtimes, or at least degradations in provided capabilities and performance, during the migration process. These concerns do not affect the system during its initial deployment.
- The time at which a component is migrated during execution must be chosen very carefully, as the component may not be in the middle of computation or interaction with another component. Again, these concerns are not applicable during the system's initial deployment.
- The added complexity of runtime redeployment, indicated in the above points, is coupled with the usually significantly reduced amount of time available to ensure that all critical system properties have been preserved. In contrast, engineers can carefully plan and analyze a system's initial deployment over a comparatively much longer period of time.

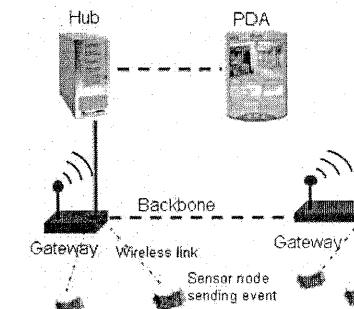
Fundamentally, the role of hardware in the context of deployment and mobility is to support a system's software architecture: the functionality embodied in processing components, the information exchanged via data components, the interactions facilitated by connectors, and the overall structure defined by the configuration. The hardware configuration can, in turn, also present constraints that must be supported by the software architecture: the choice of distribution points will induce certain architectural decisions. The deployment view of a software system's architecture can be critical in assessing whether the system will be able to satisfy its requirements. For example, placing many large components on a small device with limited memory and CPU power, or transferring high volumes of data over a network link with low bandwidth will negatively impact the system, much like incorrectly implementing its functionality will.

To illustrate these issues, consider the configuration of hardware devices shown in Figure 10-1. This configuration is typical of those used in a wireless sensor network system such as those found in many commercial buildings, power plants, and transportation systems. The sensor devices host software that can help determine the conditions of their outside environment, such as motion, vibration, fire, and moisture. Sensors are typically highly resource-constrained and can only perform minimal amounts of computation and data storage. The gateway devices aggregate, process, and can possibly share this information. They pass it on to the hubs, which may run software that can make appropriate decisions in the case of certain events or changes in system status. For example, if a gateway fails, a hub may instruct another gateway to take over the management of the "orphaned" sensors; likewise, if multiple sensors

report events of a given type (e.g., excess moisture), the hub may decide that it is appropriate to sound an alarm. Both the gateways and hubs have significantly higher capacities than the sensors, and may be able to perform large amounts of computation and/or store large amounts of data. Finally, humans can observe the system's operation via PDAs, which communicate with the hubs. PDAs are usually more capacious than sensors, but not as capacious as the hubs or the gateways. The four types of devices may all run different operating systems and other system-level software, require different dialects of programming languages, and support different network protocols.

Software engineers must take into account information such as the above when deciding how to deploy the software system onto the requisite hardware hosts. Furthermore, this information will directly impact the options an engineer has for redeploying the system's components – and possibly connectors – during runtime. The idiosyncrasies of a given platform will thus serve as software deployment and mobility constraints.

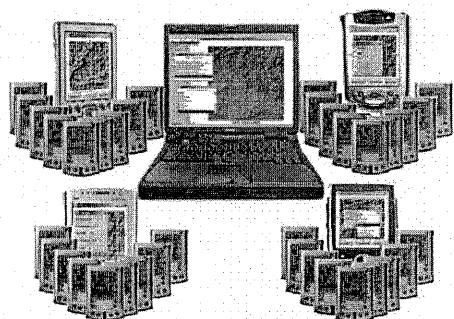
In addition to considering the characteristics of the involved hardware devices, certain application-level requirements may have a significant impact on the given software architecture's deployment and mobility. For example, the maximum allowed round-trip time between the reporting of an event by a sensor and the acknowledgment that this event has been received by an "upstream" processing component may affect where certain processing and data components are placed in the system, such as on the gateway or the hub. Such a requirement may also impact the flow of information, for instance whether and when human users need to be informed versus when the software system itself can make a decision.



**Figure 10-1.** A wireless sensor network system comprising hardware devices of several types, on which a software system is deployed.

As another illustrative example, consider an emergency response system (ERS), whose screenshot is shown in Figure 10-2. The devices in this

system are somewhat more homogeneous than in the previous example: there is a small number of powerful laptop computers, which are overseeing the overall operation; the laptops interact primarily with a set of high-end PDAs that are in charge of specific segments of the operation; in turn, each of these PDAs interacts with a large number of lower-end PDAs, which are used by individuals who participate as first-line responders. Even though they run different operating systems, each device type is capable of displaying a user interface, running Java, and communicating via TCP/IP. Therefore, aside from the computational and storage capabilities of the different devices, the number of constraints that need to be considered during a software system's deployment, and redeployment, is smaller than in the case of the wireless sensor network system from Figure 10-1.



**Figure 10-2.** An instance of the family of emergency response systems (ERS), which help with deploying and organizing teams of humans in cases of natural disasters, search-and-rescue operations, and military crises.

In this chapter we will study the impact of an explicit software architectural focus on system deployment and mobility. Conversely, we will also study the impact of deployment and mobility on software architecture. The reader should note that deployment can be viewed as a special case of mobility, that is, as the mobility of software modules *prior to* the system's runtime. The two concepts are thus closely related and many of their resulting challenges, ramifications, techniques, and tools similar.

The objective of this chapter is to define and, where necessary, clarify the role of software architecture in deployment and mobility, to discuss different approaches to software deployment and mobility, and to present a set of deployment and mobility techniques that are at an engineer's disposal. We will illustrate the main points in the discussion via examples from existing solutions. While software deployment and mobility are two important and growing areas of study, our focus here is specifically on

their architecturally relevant aspects. An annotated list of references will be given at the end of the chapter for a broader treatment of the two areas.

#### Outline of Chapter 10

10 Deployment and Mobility
10.1 Overview of Deployment and Mobility Challenges
10.2 Software Architecture and Deployment
10.2.1 Basic Concepts
10.2.2 Deployment Activities
10.2.3 Tool support
10.3 Software Architecture and Mobility
10.3.1 Basic Concepts
10.3.2 Mobility Paradigms
10.3.3 Challenges in Migrating Code
10.4 End Matter
10.5 Review Questions
10.6 Exercises
10.7 Further Reading

## 10.1 Overview of Deployment and Mobility Challenges

Modern software systems can present a number of deployment and mobility challenges. Several of these are outlined below.

1. The target processors may be geographically widely distributed, sometimes even throughout the Solar system, as is the case with some of NASA's space missions. Physically deploying the software in such settings presents logistical problems, especially if the software has to be distributed and deployed during the system's execution. For example, it may take minutes, and even hours, for the software to reach the intended target host. An accompanying concern is the security of such systems, especially during the transfer of code.
2. The target processors may be embedded inside heterogeneous devices that have different operating environments and serve different purposes. For example, aircraft, mobile robots, consumer electronic devices, mobile phones, and desktop computers present very different characteristics. A software component running on one device may not be able to run on another. Therefore, transferring a component from one such device to another may require use of sophisticated adaptor software connectors (recall Chapter 5), thus potentially affecting the system's overall performance. Such redeployments may often be impossible.

3. Different software components may require different hardware configurations for their successful execution, whether screen resolution, CPU speed, I/O devices, or memory. Again, this requires careful planning and analysis of the intended deployment profiles or runtime software migrations.
4. Typical system life spans may stretch over decades and require periodic maintenance, meaning usually that parts of the system may need to be redeployed. For example, a “buggy” component may be replaced or a more reliable connector introduced. This means that redeployment is an unavoidable activity in most software systems. It also means that, as existing components exhibit problematic behaviors, engineers may resort to migrating software to improve system performance.
5. Similarly, the deployed system is likely to evolve over time, again requiring redeployment. New functionality may be introduced and individual components or even entire hosts may be replaced with newer versions. The danger in this, as well as in the previous case, is that the deployed system’s architecture will degrade.
6. The emerging class of mobile code solutions, such as mobile agents [83], require that *running* components be redeployed from one host to another. This requires carefully assessing acceptable (partial) system downtimes and employing techniques for capturing and transferring the relevant portion of the system’s *dynamic state* in addition to the code.
7. After a component has been relocated, it must still be able to discover and access, from its new location, the system services it needs at runtime. Likewise, the rest of the system needs to be able to locate and access the services provided by that component. Selecting existing or developing new mechanisms for ensuring continuous access to system services is a major architectural consideration in mobile systems.

Traditionally the problem of mobility, and especially initial system deployment, is handled in a relatively uniform manner, and it does not always reflect the above scenarios. For example, if a Windows PC user wants to upgrade an operating system or application on his PC, or install a “patch” that will remove an existing problem, he will either obtain a CD-ROM with the needed software or go to a Web site and download the software; the user will then have to shut down all applications running on the PC in order to complete the procedure. While the PC user is controlling the deployment process, this human user-in-the-loop approach relies on certain assumptions, such as the fact that a computer’s operating environment is one of a small handful of tightly controlled environments

supported by the provider of new functionality. Regardless of a PC user’s technical prowess, he will usually have little insight into the changes done to the code running on the PC. In other words, the pre-condition for, say, installing a new spell check component into a word processor is that its user place full trust in the component’s developer, hope that the new software will work correctly, that it will eliminate any problems the user may have had with the previous spell checker, and that it will not introduce any new bugs. As we all know from experience, sometimes these patches fix the problems, and sometimes they do not, but eventually most PC users reach the point where the performance of the computer has degraded so badly that the only true remedy is to “reinstall the PC” completely.<sup>10</sup>

The situation is even more extreme if a commodity device, such as an automobile, cellular telephone, or “smart” cable TV box, begins misbehaving. In such cases, chances are that the owner or user will have to rely on a “trained professional” for a remedy. That will often require relinquishing control of the device for a period of time, during which all software running on the device will be redeployed and reinstalled from scratch, or simply replaced along with the processor on which it is running. In the process, any questions the owner or user may have about what is actually going on with his device will almost assuredly be given euphemistic non-answers because even the “trained professionals” do not understand the underlying causes, other than the fact that something in the software went awry over time.

Whatever that “something” is, it probably has underlying architectural causes. Every time a new software system is deployed on its target hosts, its initial deployment architecture is established. When that initial system is changed – via a “security patch”, by deploying a new component, or by adding a new host – its architecture also changes. If the architectural implications of those changes are not carefully analyzed and clearly understood, the system’s architecture is bound to degrade. Eventually, the architecture degrades to the point where the system is unable to function properly, requiring a complete overhaul, as in the above scenarios.

Even though the two are related, the remainder of the chapter will address separately the role of software architecture in the deployment and mobility of software systems.

---

<sup>10</sup> This phrase is sometimes used by Windows PC owners and users to indicate that the hard drive must be formatted, and the operating system, device drivers, and application programs reinstalled from scratch. Unix and Macintosh users are typically unfamiliar with such behavior.

## 10.2 Software Architecture and Deployment

Deployment is the set of activities that result in placing a given software system's components and connectors on a set of physical hosts. This set of activities can take place both during the system's construction, that is, prior to runtime, as well as during its execution. In the latter case, deployment entails the transfer and activation of components/connectors that are added to the system for the first time – in other words, either new elements or new versions of existing elements. If the elements deployed on a given host had previously been running on another host in the system, thus possibly having runtime state, that is considered to be a case of code mobility and is discussed in the next section.

In the rest of this section, we will first introduce the basic concepts underlying software deployment. We will then elaborate the set of key deployment activities with a specific focus on the role software architecture plays in them. Finally, we will discuss the tool support required of architecture-driven software deployment.

### 10.2.1 Basic Concepts

The overview of the key concepts that underlie software deployment, provided in this section, draws from a deployment technology characterization framework by Carzaniga, Fuggetta, Hall, Heimbigner, van der Hoek, and Wolf [35].

A software system is deployed on one or more hardware devices, referred to as *hosts* or *sites*. Each site provides a set of *resources* needed for hosting and executing the system or some of its subsystems. The resources include the different elements of

- the hardware architecture (e.g., memory, CPU),
- the network architecture (e.g., available protocols, IP port numbers),
- the peripheral devices (e.g., hard disk, keyboard),
- the system software (e.g., operating system, device drivers, middleware),
- other application-level software (e.g., GUI builders, databases), and
- the data resources (e.g., data files, Globally Unique Component Identifiers or GUIDs).

Resources can be either *exclusive* (e.g., IP port number, GUID) or *shareable* (e.g., CPU, data file).

A software system is composed from a specific set of components and connectors, with carefully prescribed interconnections and allowed interactions. Multiple versions of the components and connectors may exist, meaning that the system itself may have multiple versions as well. A

*version* is defined to be a time-ordered revision, a platform-specific variant, or a functional variant.

Initial system deployment involves the transfer of system components or connectors from one or more *source* or *producer* hosts to one or more *destination* or *consumer* hosts. Subsequent deployment activity will typically involve introducing new functionality (that is, new components) to the system, or replacing existing components or connectors with different versions.

### 10.2.2 Deployment Activities

Architecture-driven software deployment comprises a process that must be carefully *planned*, *modeled*, *analyzed*, and finally *effected* or *executed*. We will discuss these four activities in more detail below. We will specifically focus on the relationship between each activity and software architecture.

#### Planning

It is critical that the deployment of a software system be carefully planned. Many important system properties, particularly in a distributed setting, will be affected by the system's deployment. For example, the system's latency in delivering a given service can be improved if the system is deployed such that the most frequent and voluminous interactions required for that service occur either locally or over reliable and capacious network links.

For any large, distributed system, many deployments—that is, mappings of software components and connectors onto hardware hosts—will be possible in principle. Some of those deployments will be more effective than others in ensuring the desired system properties, such as its dependability, availability, security, and fault-tolerance. A system that meets its requirements and possesses these properties is said to deliver a desired level of service quality, most often referred to as QoS for “quality of service”, to its users. Of course, in order to be able to claim that the system delivers the required QoS, the different QoS dimensions must be measurable and quantifiable. We will revisit this issue in the next section. In the remainder of this section, we will assume that the QoS dimensions in question are, in fact, measurable and quantifiable.

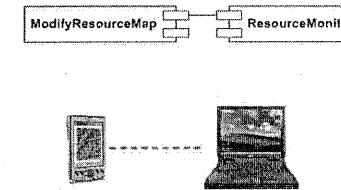
It should be noted that there are cases in which the deployment decisions can be and are made with relative ease – regardless of whether they are actually a good fit for the given system or not. One example is a typical desktop environment, in which a human user decides what software he wants installed on his personal computer. Another example would be a system deployed by a space agency, comprising an inter-planetary probe

and a ground station. In such systems, it is typically known *a priori* on which “side” (flight or ground) the system’s different components will reside. Yet another example, to an extent, is the wireless sensor network system depicted in Figure 10-1: the GUI components implemented in Java will reside on the PDAs, while the computationally intensive components implemented in C++ will be deployed to either the hubs or gateways [181]. While the potential presence of multiple hubs and gateways, and multiple types of PDAs, will still require that the system’s architects and engineers consider the effects of their deployment decisions within each class of components (in this example, GUI components and computationally intensive components, respectively), the number of possible deployments is significantly reduced.

The deployment problem is substantially more challenging in a system such as the one depicted in Figure 10-2, in which the number of hardware hosts is significantly larger and all devices provide roughly similar execution environments (in this case, Java). The problem of determining an effective deployment becomes intractable for a human engineer if, in addition to this, multiple QoS dimensions such as latency, security, availability, and power usage, must be considered simultaneously, while taking into account any additional constraints. For example, component X may not be deployed on hosts Y and Z because of the component’s size, the hosts’ inability to provide the resources necessary for its execution, security concerns, or something else. This is a particularly challenging problem because of the following:

- A very large number of system parameters influence the QoS dimensions of a software system. It may be possible to identify a subset of system parameters, such as network bandwidth, network reliability, and frequencies of component interactions, that influence the majority of QoS dimensions; however, it may not be possible to identify all of them.
- Many services provided by a system and their corresponding QoS influence the system users’ satisfaction.
- Different service qualities may be conflicting, that is, improving one may degrade another. A simple example is security and efficiency: if the system’s designers elect to use powerful encryption facilities for all network traffic, such a decision will very likely have a direct, negative, impact on the system’s performance.
- The space of possible deployment architectures for a given software system is exponentially large.

In general, for a system comprising  $c$  software components and connectors that need to be deployed onto  $h$  hardware hosts, there are  $h^c$  possible deployments. Clearly, some of those deployments may not be valid due to location constraints such as those mentioned above, memory restrictions on different devices, network bandwidth considerations, or availability of hardware and system software. This will reduce the space of possible deployments. On the other hand, the human user will still be tasked with determining which deployment he prefers, why, and, in the process, may have to consider multiple invalid deployments.



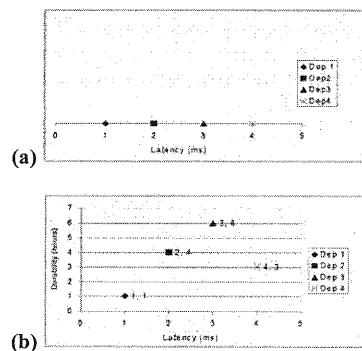
**Figure 10-3.** A small subset of the ERS system’s architecture, comprising two software components and two hardware hosts. The components are depicted in UML for convenience.

As a simple example, consider the following scenario. A very small subset of the ERS system’s architecture sketched in Figure 10-2 is depicted in Figure 10-3. This particular system contains only two software components and two hardware hosts; the connector enabling the interaction between the two components has been elided for simplicity. The two components interact to provide a *Schedule Resource* service, and the only property (that is, QoS dimension) of interest is latency. This small system has four possible deployments:

1. Both components are deployed on the PDA.
2. Both components are deployed on the laptop.
3. *ModifyResourceMap* is deployed on the PDA, while *ResourceMonitor* is deployed on the laptop.
4. *ResourceMonitor* is deployed on the PDA, while *ModifyResourceMap* is deployed on the laptop.

For such a small system, it is, in fact, possible to consider all of the possible deployments and to measure their actual latency. Let us assume that the measured latencies of the four deployments are as shown in Figure 10-4(a). These values are hypothetical, used here for illustration only. From this data, it is easy to determine that the first deployment exhibited the shortest latency and is thus the optimal deployment.

**Figure 10-4.** Evaluating deployments of the ERS subsystem from Figure 10-3. (a) Latency is the only QoS dimension of interest. (b) Latency and durability are the QoS dimensions of interest.

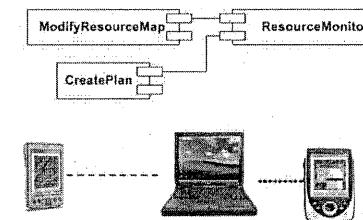


Let us now extend the example slightly and introduce another QoS dimension – durability. We define durability as the inverse of the system's rate of energy consumption. In many embedded and mobile settings, systems with higher energy consumption rates will run out of battery power sooner, that is, they will have lower durability. Therefore, deployments that reduce the energy consumption rate will increase the system's durability.

Figure 10-4(b) shows the (hypothetical) durability values plotted alongside the previously obtained latency values. The first deployment still exhibits the shortest latency, but the third deployment is most durable. This phenomenon is known as *Pareto optimal* in multi-criteria problems such as this one: no single deployment can be considered optimal unless additional criteria are introduced that will allow an architect to reconcile the two competing deployment options. In this example, if the system's stakeholders deemed durability more important than latency, the third deployment would likely be selected over the first one. However, even if there is no such additional criterion, the architect still has all relevant data available and can make the decision(s) he deems most appropriate.

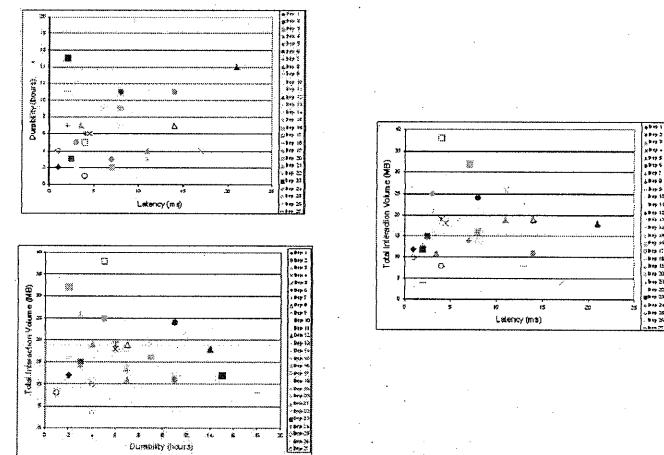
To illustrate how quickly this problem becomes intractable, let us consider a slightly expanded scenario, depicted in Figure 10-5: this subsystem of the ERS has three components and three hosts. Even though it does not directly impact the discussion below, for the sake of completeness it should be noted that this three-component system provides an “exchange plan” service as well as the “schedule resource” service. Furthermore, there are now three QoS dimensions of interest: in addition to minimizing latency and maximizing durability, the system must also minimize the total volume of data exchanged across the network.

**Figure 10-5.** A slightly larger subset of the ERS system's architecture, comprising three software components and three hardware hosts.



This system has 27 possible deployments ( $3^3$ ). For each of those deployments, let us assume that the three QoS properties have been measured or estimated. Visualizing the 27 data points in a single three-dimensional diagram would be possible, though difficult. Note that visualizing software deployment scenarios with greater numbers of components and hosts, and especially with four or more QoS dimensions, in a single diagram would be essentially impossible. Instead, architects would most likely plot separate two-dimensional diagrams to study the relationships between pairs of QoS dimensions. The three such diagrams for the scenario from Figure 10-5 are shown for illustration in Figure 10-6.

**Figure 10-6.** The pairwise trade-offs among the three QoS of interest (latency, durability, and interaction volume) for the ERS subsystem shown in Figure 10-5.



It should be obvious from this example that, even for a system that is as small as the one depicted in Figure 10-5, manually calculating the QoS values of individual deployments and then determining the best deployment from those values is infeasible. Therefore, a solution that

meets the challenges identified above and allows a software system's architects to plan the system's deployment appropriately will need to (1) provide an extensible model that supports inclusion of arbitrary system parameters; (2) support definition of new QoS dimensions using the system parameters; (3) allow users to specify their QoS preferences; and (4) provide efficient and generic algorithms that can be used to find a solution (i.e., deployment architecture) which maximizes the users' satisfaction in a reasonable amount of time.

This solution is amenable to implementation, alleviating at least some of the architect's responsibility. In turn, this allows architects to focus on tasks such as specifying concrete targets for QoS dimensions of interest, rather than the menial but critical ones such as determining whether a given deployment satisfies all of the system constraints and, if so, calculating the values of its various QoS dimensions.

For example, in the case of the scenario from Figure 10-5 and Figure 10-6, the architect may be interested in a deployment with specific latency, durability, and interaction volume thresholds. Manually determining and analyzing each individual deployment that is possible, that is, that satisfies all system constraints, and choosing one that in fact meets the set thresholds, would be overly time consuming (it could take hours for this small scenario and years for even only slightly larger systems) and error prone. Furthermore, the architect will likely elect to stop once he has found the first deployment that meets the desired criteria. In contrast, a software-based solution working on the same problem would likely be able to determine a number of valid deployments that meet the QoS criteria, and choose the best one.

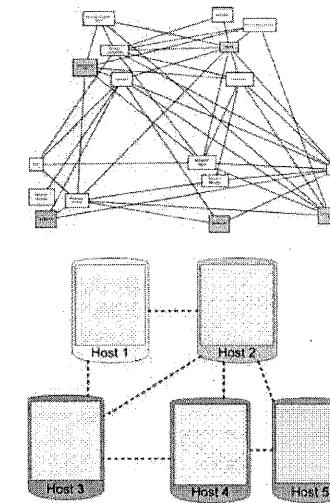
Automated support for deployment modeling and analysis would also allow architects to study, and quantify, any changes in a system's runtime behavior. In turn, this would allow them to formulate plans regarding whether and when to redeploy the system or some of its parts.

### Modeling

In order to be able to make and effect a deployment plan for a large, long-lived, distributed software system, the system's architects first need to create a detailed model comprising all concerns pertaining to the system's deployment. This is an example of several concerns pertaining to the system's hardware and network infrastructure permeating the space of principal design decisions, that is, the system's software architecture.

Consider the two diagrams in Figure 10-7, corresponding to a subset of the ERS application depicted in Figure 10-2: the top diagram shows a high-level view of the ERS system's architectural configuration, while the bottom diagram shows the configuration of the hardware hosts on which the software is to be deployed. For simplicity, the top diagram does not

show any software connectors. Instead, all interaction paths among the components are represented simply as lines. The reader can choose to interpret them as procedure calls for the purpose of the ensuing discussion. The dashed lines in the bottom diagram depict network connectivity.



**Figure 10-7.** The software architectural configuration of a subset of the ERS application (top) and the hardware configuration on which the software is to be deployed.

In order for a software architect to determine what an effective deployment of ERS's software components to its hardware hosts would be, he would need a lot more information than is contained in the two diagrams in Figure 10-7. For example, the architect would need to know how computationally intensive the *Deployment Advisor* component is; how large the *Repository* is; how frequently the *Clock* component updates the remaining components in the system; what type of GUI facilities the five *UI* components in the system require; and so on. Furthermore, the architect would need to know many of the characteristics of the five hosts (e.g., their capacities, available peripheral devices, system-level software running on each, and so on) as well as the network links connecting them (e.g., the available bandwidth, protocol, link reliability, and so on). Only after all of this information is available, can the architect make appropriate deployment decisions.

Therefore, an effective deployment model requires the following elements:

- software system elements (components and connectors), their configuration, and their parameters;
- hardware system elements (hardware hosts and network links), their configuration, and their parameters;
- any constraints on the system elements and/or their parameters; and
- formal definitions of QoS dimensions of interest.

In order to be able to make appropriate decisions in situations in which multiple deployment options are acceptable, the architects may also need to represent system users or user types and their preferences.

For any moderately-sized software system, the above model can be very large, especially if architects decide to capture many parameters and constraints of the overall system and its individual hardware and software elements. Example parameters of a software component are the CPU and memory requirements for the component's execution, characteristics of the required execution substrate, such as the needed version of the Java Virtual Machine, and so on. Likewise, for a connector enabling the interaction of two or more components, the system model would encompass many of the same parameters as in the case of components, but would also capture parameters such as the sizes and frequencies of the interaction between the components, security mechanisms available, and whether the connector assumes a particular distribution profile (e.g., single address space, inter-process, network-based).

Even though the primary responsibility of a software architect is to focus on a system's software aspects, in the case of deployment modeling software architects must also consider the characteristics of the hardware platforms and the network. Extensible architecture descriptions languages such as xADL, AADL, and even UML, discussed in Chapter 6, are able to or already incorporate such modeling elements.

There may be many constraints specified on the software and hardware elements of a deployment model. For instance, *location constraints* may specify the relationship between software and hardware elements: requiring, allowing, or prohibiting that certain elements be deployed on certain hosts. In the example from Figure 10-7, it may be required that the *Clock* component reside on *Host 2*, while the *Repository* component may be prohibited from residing on that host.

*Collocation constraints* specify groups of components and connectors that need to be deployed, and re-deployed, as a collection, as well as groups of components and connectors that may not be deployed on the same host. For example, another way of specifying the above two location constraints for Figure 10-7 would be to couple the *Clock* component's location

constraint (that it must reside on *Host 2*) with a collocation constraint stating that the *Clock* and *Repository* components may not reside on the same host.

Beyond location and collocation, other constraints may restrict the versions of software connectors that may be used to enable the interactions of specific versions of components; the hardware configurations that are required or disallowed for deploying a given component; and so on.

A final, critical facet of a deployment model is a quantification of the QoS dimensions of interest. If a given system property cannot be quantified, it cannot be estimated or measured precisely, nor can the impact on that property of a system's particular deployment be assessed objectively. Thus, for example, trying to determine a deployment of the ERS that will optimize its usability would be inherently difficult: usability is a largely subjective notion that depends on many, sometimes implicit and possibly ill understood, factors.

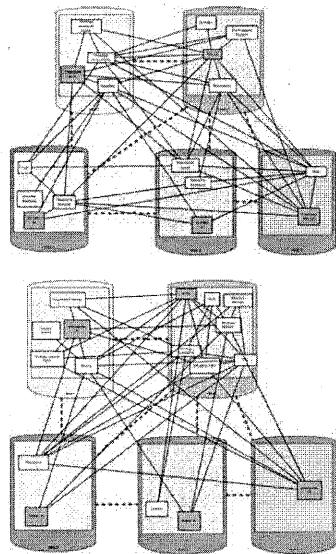
Fortunately, many important system properties can be quantified: reliability, availability, size, energy consumption rate, latency, and data volume are examples. Some of these properties may have multiple interpretations, which will differ across architects, projects, and organizations. Nonetheless, in principle it is possible to select a specific definition for a given property. Thus for example, one possible definition of availability for a system service (e.g., *Schedule Resource* discussed in the context of Figure 10-3) may be as the ratio of the successfully completed service requests to the total number of attempted service requests. It is not critical that this be the only, or the best, definition of availability. It is much more important that the definition fits the needs of the project in question, and that it is applied consistently.

### Analysis

Developing a detailed deployment model will be a sizeable, human-intensive task for any large, distributed application: many parameters of many system elements will have to be modeled; many constraints will have to be captured; QoS dimensions of interest will have to be formally defined; system users and their preferences will have to be modeled; and so on. Doing all that will be worthwhile only if the model is used effectively to make the necessary, complex deployment decisions. To that end, the system's deployment model will have to be *analyzed* for properties of interest.

Consider for illustration the two diagrams in Figure 10-8. Both represent deployments of the ERS application's software elements onto its hardware nodes. The connectivities of both the software and the hardware configurations in the two Figure 10-8 diagrams are identical to those depicted in Figure 10-7. In other words, the applications corresponding to

the two deployments are functionally equivalent to each other. The only difference between the two diagrams is that some of the software elements have been repositioned across the hosts. Using the terminology introduced in Chapter 3, we can then say that the two diagrams represent different candidate deployment views of the ERS application's architecture.



**Figure 10-8.** Two possible deployments of the subset of ERS depicted in Figure 10-7.

An architect considering these two candidate deployments will have to make certain determinations.

1. First, are both deployments valid? That is, do they satisfy all ERS system constraints?
2. Secondly, which of the two deployments is “better”?
3. Finally, once the better deployment is selected, does that deployment exhibit acceptable properties, or must an even “better” deployment must be found?

Answering the first question —Is the deployment valid?— is relatively easy. If the system constraints have been specified rigorously, then this becomes a straightforward constraint satisfaction problem.

The answer to the second question —Which deployment is better?— is more uncertain. In order for the architect to answer that question, he must have a clearly defined measure of goodness for a system's deployment. That means that the system's deployment model will need to provide definitions of all QoS dimensions of interest. In turn, these QoS dimensions will have to be measured, or at least estimated. If multiple QoS dimensions are under consideration, as will be the case with most all large systems, the architect will very likely have to deal with Pareto optimal situations (recall Figure 10-4b): one deployment may prove superior with respect to one subset of the QoS dimensions, while another deployment is better with respect to a different subset of the QoS dimensions.

For this reason, additional criteria will have to be introduced into the model. One possibility is to rank the QoS dimensions. For example, it may be decided that durability is more critical than latency. In that case, the third deployment from Figure 10-4b would be selected.

Another possibility, as suggested previously, is to introduce system users into the deployment model and capture their preferences explicitly. For example, one user could state that high durability of the *Schedule Resource* service in the ERS system is more important, by a given quantified factor, than its low latency; another user may specify another, possibly clashing preference. This would allow the architect to introduce the notion of the system's *utility* and select the deployment that provides the greatest total utility to all the users, or alternatively, the deployment that provides the greatest utility to the most important user or users.

One of the frequently used “axioms” of software systems engineering is:

**Better-cheaper-faster – pick any two.**

This means that for any software system, only two of these three properties can be achieved at one time. For example, it is possible to construct a high-quality system (“better”) that delivers its functionality efficiently (“faster”), but that will be a costly enterprise (“cheaper”) is sacrificed. Likewise, if we want an inexpensive system (“cheaper”) that is also highly performant (“faster”), we should expect the system's quality (“better”) to be compromised.

There are alternative ways of stating this principle. For example:

**Functionality-scalability-performance – pick any two!**

All of the various incarnations of this principle point to the inherent trade-

**Better-Cheaper-Faster  
– pick any two!**

offs among the properties in a software system.

Relating this to the deployment problem, it should not be surprising to a software engineer that every system user will not be able to have all of his preferences satisfied in a chosen system deployment. This will be the case for even those users who are deemed “very important”. Large, distributed software systems such as the ones that are being discussed here are multi-faceted and involve many trade-offs, such as those mentioned above. Thus, a system’s user will not be able to expect realistically that the system will deliver its services in the optimal (for that user) fashion. Rather, the best one can hope for when addressing the system deployment problem is that the sub-optimality in the system’s delivered QoS will be minimized.

Another way of looking at this is that, when making deployment decisions, some or even all of the system’s users are likely to be unhappy with the system. This stems directly from the “better-cheaper-faster” axiom. The software architect’s job is to use the concepts provided in this chapter to minimize that unhappiness.

Answering the third question —Is there a better deployment than the current one?— can be very challenging. It may require considering a very large number of deployment options and for each of them establishing the deployment’s validity and comparing the new deployment to the existing one. This question is closely related to a more general question —What is the best deployment possible for a given system?— which is infeasible to answer in the general case because of the deployment problem’s exponential nature.

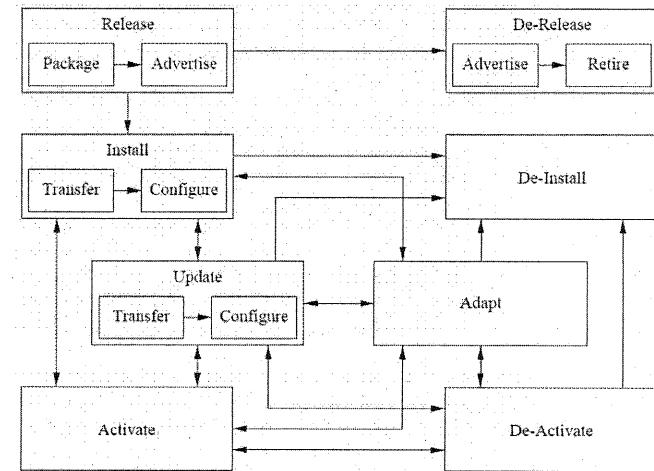
There is a class of algorithms that can be applied to questions such as these. As stated above, the deployment problem is an instance of a multi-dimensional optimization problem. Techniques such as mixed-integer linear programming (MIP) and mixed-integer non-linear programming (MINLP) are frequently used to solve such problems [201]. The main shortcoming of MIP is that it searches exhaustively for the best solution to a problem, and is thus inapplicable to even moderately large deployment scenarios. MINLP algorithms in turn provide approximate, rather than an optimal, solutions. Furthermore, MINLP algorithms may not always converge on a solution.

There are other heuristic-based strategies that can be applied to solving complex problems such as this, such as greedy, genetic, and decentralized strategies [181]. However, none of those strategies can guarantee that the suggested deployment is the optimal one. In the case of the simpler formulation of the third question —Is there a better deployment than the

current one?— this may result in failing to identify it even though many such deployments may exist. In the case of the question’s more general formulation —What is the best deployment possible for a given system?— this may result in selecting a deployment that is actually suboptimal but is the best deployment the chosen algorithm can find.

### Implementation

Once the deployment problem has been modeled and a specific software system’s deployment suggested in the manner outlined above, that deployment needs to be effected. As noted by Hall et al. [109, 110] and Carzaniga et al.[35], some of the activities in a software system’s deployment process take place on the host that is the source of the deployed component, while other activities take place on the host that is the destination of the deployed component. Source hosts are also referred to as producers, while destination hosts are referred to as targets, or consumers. The overall relationship among these activities is shown in Figure 10-9. We will briefly discuss each of these activities below, with a particular focus on the role of software architecture in the deployment process.



**Figure 10-9.** Software deployment process: deployment activities and their relationships. The diagram has been adopted from [35].

**Release** — A software system’s release is the initial activity in that system’s deployment process. It takes place on the producer site, or sites, after the system’s development has been completed. The system is *packaged* so that it can be transferred to the consumer sites. In certain settings (e.g., desktop computing) the system may need to be *advertised* to

potential consumers. The packaged system will typically contain the following:

1. the system's description, including its software architectural configuration, dependencies on system-level facilities and any external components, and requirements specific to individual software system elements and the entire system;
2. all of the necessary software modules – both the application and any “helper” components necessary for the released application’s correct execution;
3. a deployment model indicating which components need to be deployed on which processes and/or hosts;
4. the deployment procedures that must be effected on the consumer sites in order to extract and deploy the software system from the release package; and
5. any additional information that is needed to manage the system at the consumer sites, such as the necessary periodic updates to the data used by the system and expected downtimes for specific system services.

**Install** – Once the system has been packaged at the producer sites and transferred to the consumer sites, it is ready to be configured and installed for operation. Installation is a complex activity that encompasses all of the steps necessary to enable the system to execute. In other words, installation deals with

1. extracting from the deployment package the system’s description, including its software architecture and deployment models;
2. based on those models, assembling all of the system’s elements – both the application-level components as well as any accompanying utilities;
3. ensuring that all the resources needed for the system’s correct operation are available and properly configured; and
4. establishing any required conditions on the target hosts, such as setting any global system variables, establishing the needed directory structures, and setting up the appropriate classpaths.

**Activate** – Once the system is installed, it needs to be activated for use on the target hosts. Activation consists of providing a command, or sequence of commands, that will be required to start up the system.

**Deactivate** – Deactivation involves disabling and/or shutting down a system, or any of the system’s facilities that are still active on the target hosts.

**Update** – Once a system has been installed and activated on the target hosts, it may need to be updated for different reasons over time. Updates are initiated by the system’s producers, and involves the same activities as

the system’s original installation, with the caveat that only the necessary subset of the system is packaged and received from the producer hosts. The system may need to be deactivated before it is updated, and then reactivated thereafter. Alternatively, the system may support dynamic re-deployment (recall the above discussion as well as see Chapter 14). It is critical that the software system’s update be properly reflected in its architectural models. If this is not ensured, the architecture will degrade and any subsequent updates may result in system defects.

**Adapt** – Adaptation encompasses a wide range of activities that result in changing the system, possibly dynamically, in response to events in the system’s execution environment. Adaptation is an important aspect of architecture-based software development, thus Chapter 14 is dedicated to it. With respect to software deployment, adaptation can result in the system’s re-deployment (that is, repositioning of its software components across execution processes and/or hardware hosts). Adaptation will be further discussed below in the context of mobility.

**De-Install** – If the system is no longer needed on the consumer sites, it will need to be removed. A simple view of de-installing a system is that it simply reverses the steps taken during the installation. However, any subsequent updates and adaptations must also be taken into account, as must any dependencies other systems on the given consumer host have to the system being removed. This is why it is critical to maintain current architectural models for all deployed software systems. It should also be noted that, before the system is de-installed, it may need to be deactivated first.

**De-Release** – After some time, the producer of a given system may decide not to support the system any longer. In other words, the producer may decide to retire the system. This may be because one or more of the system’s subsequent versions are superior, the market size for the product is too small, the producer has discontinued the product, or the producer has gone out of business. The withdrawal of the producer’s support for the system is usually advertised. The system’s consumers can then decide whether they still want to use the system, with the accompanying risks, or to de-install it.

### 10.2.3 Tool support

In order to properly support the software architecture-based deployment modeling, analysis, and implementation activities discussed above, engineers must be supplied with appropriate software tools. Some of those tools, such as those for software installation, are widely used. For example, most all desktop software comes with an installation wizard. Tools for other activities are not as prevalent. Furthermore, they frequently fail to consider the system’s software architecture. This carries

the risk that important architectural concerns will be missed during deployment and re-deployment. It also carries the risk that key architectural design decisions will be violated.

Ideally, a deployment tool set will enable architects to

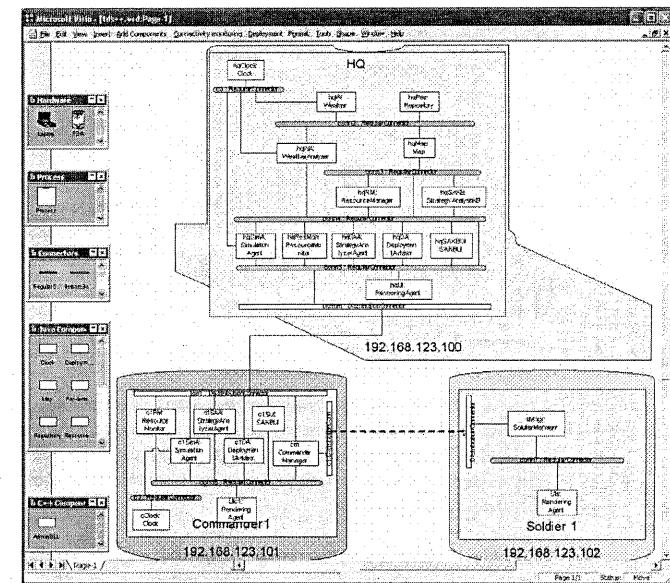
1. *model* in detail the software system's deployment concerns,
2. *analyze* the deployment model for desired properties,
3. *effect or implement* that deployment model,
4. actively *monitor* the system for properties of interest, and
5. *update or adapt* the system as a result.

While there exist tools that support many facets of the above activities (e.g., Software Dock [110]), they frequently take an implementation-centric, rather than a software architecture-centric view of the deployed system. Here we will briefly focus on a couple of examples of architecture-based deployment tools.

An example of an integrated tool set allowing several of these activities to take place seamlessly for the ERS application family is shown in Figure 10-10. The environment allows an architect to graphically model certain aspects of a system's deployment:

- software components and connectors, as well as the locations of their implementations in Java and/or C++;
- their connectivity in the particular application's architectural configuration;
- hardware nodes and their IP addresses; and
- the physical network's connectivity.

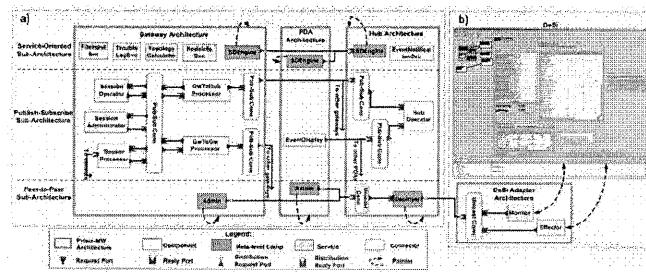
Once the model of an application's deployment is completed, this tool is capable of releasing and installing the application, as well as monitoring it during runtime. For example, the screenshot in Figure 10-10 shows that the network link between the two PDAs is down.



**Figure 10-10.** An example architecture-based software deployment environment. An application is modeled as a collection of software components and connectors, as well as hardware hosts and network links. The network link between the two bottom hosts is temporarily down (denoted by the dashed line).

A more sophisticated distributed system deployment tool, called DeSi [179], is depicted in Figure 10-11b. DeSi allows an architect to provide a more extensive model of the system's deployment, such as that discussed earlier in this chapter. The tool also is able to analyze the model and suggest an effective deployment for a given system, which will ensure the system's key QoS dimensions. An example deployment for an application is shown in Figure 10-11a. Interested readers can refer to [181] for further details of this particular application. Finally, the tool is able to interact with the system's implementation platform, observe, and analyze any changes in the system's operating conditions. In response, DeSi reevaluates the deployment view of the system's current architecture, and may suggest and effect an improved one.

**Figure 10-11.**  
 (a) A deployment view of a software system distributed across three types of devices.  
 (b) A deployment modeling and analysis tool that interacts with the system at runtime to ensure the preservation of its key properties.



## 10.3 Software Architecture and Mobility

Once a software system is in operation, parts of it may need to be re-deployed, or migrated, in response to changes in the runtime environment or the need to improve certain non-functional properties of the system. The re-deployment of a software system's components is a type of software system *mobility*.

Mobility is an area that has received significant attention recently. This chapter will focus specifically on those aspects of mobility that are relevant to a software system's architecture. The reader should note that, in order for software mobility to be possible, certain low-level system implementation facilities, such as dynamically linked libraries and dynamic class loading, usually must also be available. We will not focus on such facilities here as they are outside the scope of this book.

### 10.3.1 Basic Concepts

*Mobile computing* involves the movement of human users together with their hosts across different physical locations, while still being able to access an information system unimpeded. This is also referred to as *physical mobility*. Such mobile computing need not necessarily involve the mobility of software systems, or portions of them, from one host to another. If a piece of software moves across hardware hosts during the system's execution, that action is referred to as *code mobility*, or *logical mobility*.

If a software module that needs to be migrated contains runtime state, then the module's migration is known as *stateful mobility*. If only the code needs to be migrated, that is known as *stateless mobility*. Clearly, supporting stateful mobility is more challenging since the mobile component's state on the source host need to be captured, migrated, and reconstituted on the destination host. Furthermore, the component may be

moved only at certain times (e.g., when it is not operating on its internal state, that is, when it is quiescent [154], as discussed in Chapter 14). Finally, the effect of the component's migration, and thus its temporary downtime, on the rest of the system and its dependence on the component's internal state must be considered. This is why Fuggetta, Picco, and Vigna [83] refer to stateful mobility as *strong mobility*, while they consider stateless mobility to be *weak mobility*.

### 10.3.2 Mobility Paradigms

It is widely accepted that there are three general classes of mobile code systems: remote evaluation, code-on-demand, and mobile agent [83]. These are typically distinguished from "fixed" code paradigms such as client-server. In a client-server system, the server has both the logic and the resources needed for providing a given service. On the other hand, the distribution of the know-how and resources varies across the mobile code paradigms.

#### Remote Evaluation

In remote evaluation, a component on the source host has the know-how but not the resources needed for performing a service. The component is transferred to the destination host, where it is executed using the available resources. The result of the execution is returned back to the source host.

In the terminology used previously in this chapter (that is, from a software architectural perspective) this means that a software component is

1. re-deployed at runtime from a source host to a destination host,
2. installed on the destination host, ensuring that the software system's architectural configuration and any architectural constraints are preserved,
3. activated,
4. executed to provide the desired service, and
5. possibly de-activated and de-installed.

#### Code-on-Demand

In code-on-demand, the needed resources are available locally, but the know-how is not. The local subsystem thus requests the component(s) providing the know-how from the appropriate remote host(s).

From a software architectural perspective, code-on-demand requires the same steps as remote evaluation; the only difference is that the roles of the target and destination hosts are reversed;

#### Mobile Agent

If a component on a given host (1) has the know-how for providing some service, (2) has some execution state, and (3) even has access to some, though not all, of the resources needed to provide that service, the

component, along with its state and local resources, may migrate to the destination host, which may have the remaining resources needed for providing the service. The component, along with its state, will be installed on the destination host and will access all of the needed resources to provide the service.

As mentioned above, from a software architectural perspective, mobile agents are stateful software components. Therefore before the steps outlined above are taken, a mobile agent must first be safely de-activated and possibly de-installed from the source host. This may pose certain challenges, which will be further discussed next.

### 10.3.3 Challenges in Migrating Code

Runtime mobility of software depends on several factors that are not architectural in nature. For example, the runtime platform must be able to support dynamic loading and linking of code modules. Likewise, both the source and target hosts must provide all of the software and hardware utilities necessary to execute the code.

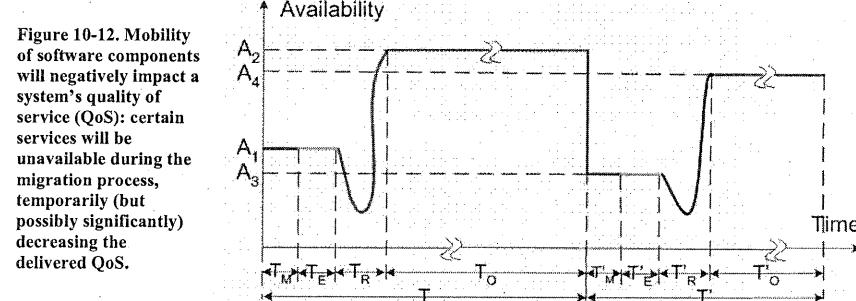
At the same time, there are architectural concerns of which engineers must be aware. One such concern is quiescence. It may be unsafe to attempt to migrate a software component in the middle of processing, while it is waiting for a result from another component, or while other components are requesting its services. Therefore, the system must provide facilities that allow temporary suspension of all interactions originating from or targeted at the component in question, until the component is relocated to a new host.

In general, quiescence requires at least two capabilities. The first one must be embodied in the component itself, allowing the system to instruct the component to cease any autonomous processing, and later on to restart it. The second capability may require that special-purpose elements, such as adaptor connectors, be inserted into the system temporarily, to insulate the component from outside requests. These modules may also log the received requests and route them for processing after the component has been migrated.

Another important issue concerns the system's provided quality of service as a result of code mobility. Consider the example of Figure 10-12. The postulated system provides a given level of availability for its services. The system is monitored for a time,  $T_M$ , and it is established that the provided availability is  $A_1$ . If the system's stakeholders wish to improve the system's availability to a higher level  $A_2$ , e.g., by migrating one or more of its components to different hosts, they will first evaluate, during time  $T_E$ , where those components should reside. This evaluation can be accomplished by using a deployment analysis capability such as those

discussed previously in this chapter. Once the target hosts have been determined, the mobile components are rendered quiescent, packaged for re-deployment, and migrated to their target hosts. Once they are installed on the target hosts and activated, the system indeed operates at availability level  $A_2$  during the next time period  $T_o$ .

The system will operate at this availability level until some change occurs in the system itself—e.g., a software or hardware failure—or in the physical environment—e.g., emergence of obstacles. Such changes may cause the availability level to decrease to some level,  $A_3$ , as shown in the right portion of Figure 10-12. The above process will then need to be repeated in order to improve once again the system's availability to an acceptable level,  $A_4$ . This pattern may occur many times during a mobile system's execution.



**Figure 10-12.** Mobility of software components will negatively impact a system's quality of service (QoS): certain services will be unavailable during the migration process, temporarily (but possibly significantly) decreasing the delivered QoS.

But what about the time period  $T_R$  needed to effect the re-deployment? Since one or more system components were inaccessible, the system's quality of service may have gone down significantly. In fact, it is possible that the “dip” in availability, however temporary, may be unacceptable to the system's users. In that case, migrating the components in question will not be the best approach, and other dynamic adaptation techniques (e.g., component replication with continuous state synchronization) may need to be considered. Dynamic adaptability of software system architectures is treated in Chapter 14.

### 10.4 End Matter

System deployment and mobility are critical needs in today's long-lived, distributed, pervasive, and embedded software systems. The nature of such systems demands that the past assumptions and techniques, employed particularly in the domain of desktop computing, be reassessed. The

complexity of these systems also mandates that deployment and mobility be considered from a software architectural perspective. While many facets of both deployment and mobility depend on implementation and low-level system issues, they are significantly impacted—and significantly impact—a given system's software architecture. This chapter has identified a number of pertinent concerns and suggested strategies for addressing them.

The perspective on software architecture we have adopted in this book—that it is a set of principal design decisions about a software system—directly and naturally enables an architect to embrace deployment and mobility, and exert control over their relevant facets. The modeling and analysis of deployment and mobility at the architectural level helps to ensure the system's proper functionality and desired quality attributes. Moreover, maintaining the relationship between the system's architectural model and its implementation allows system monitoring to be reified into architectural (re)deployment and mobility decisions, which are then effected on the running system. By broadening the notion of software architecture to encompass an area that has traditionally been considered outside its scope, software architects can gain significant added leverage in stemming architectural degradation.

In addition to the architecture-focused concerns discussed in this chapter, many non-architectural issues are pertinent to deployment and mobility as well. Further Reading, discussed below, provides pointers to some of the relevant literature.

**The Business Case**

Dynamism in the form of deployment and mobility is a fact of life in modern systems. It is impractical, often unacceptable, for many of today's systems to have static configurations, or to be brought down for upgrades. Moreover, deploying a system in a manner that ensures its key properties and satisfies all of the constraints placed on it is a difficult, perhaps even impossible, task for a human engineer. Modeling and analyzing the appropriate concerns at the architectural level provides at least some added leverage, and can help answer many questions before significant resources are invested into supporting the required low-level deployment and mobility facilities.

At the same time, supporting deployment and mobility at the level of architecture requires a lot of careful preparation, as was indicated in this chapter in the case of deployment modeling. It also requires keeping a close watch on the architecture. Even more dangerous and costly than "diving" into low-level system details right away would be the architecture's degradation. The observation repeated throughout this book applies in this case as well: the benefits, monetary and otherwise, of an

architecture-based software development philosophy can be reaped only if the architecture remains the linchpin of all development activities, including the deployment and post-deployment activities.

## 10.5 Review Questions

1. What is deployment?
2. What is mobility?
3. How are deployment and mobility related to and different from one another?
4. Discuss the challenges in determining the optimal deployment for a software system.
5. How can software architecture aid in addressing those challenges?
6. Which facets of a system should be modeled in order to solve the deployment problem?
7. Which, if any, of those facets fall outside the realm of software architecture, and why?
8. What is Pareto optimal?
9. Name and describe the different deployment activities.
10. Which activities take place on the source hosts, and which ones on the target hosts?
11. What is the difference between physical and logical mobility?
12. What is the difference between stateful and stateless mobility? Which is more challenging to realize?
13. What is remote evaluation? What steps does it require?
14. How is remote evaluation different from code-on-demand?
15. How do mobile agents work?
16. Describe quiescence and the challenges it entails.
17. Discuss the impact of mobility on a system's provided quality of service.

## 10.6 Exercises

1. Select one of the implemented Lunar Lander applications from Chapter 9 and deploy it on (a) a single host and then (b) at least two hosts. Discuss the issues you encountered.
2. In what ways would the knowledge that an application, such as Lunar Lander, may need to be deployed on multiple hardware hosts impact its design? For example, would the design of Lunar Lander from Figure 8 in Chapter 9 be any different if the architects had known that the *GUI* component would need to run on a separate host from the remaining components?

3. Leverage the Lightweight C2 framework discussed in Chapter 9 in providing runtime mobility support for the implemented Lunar Lander application. Develop and execute a mobility scenario. Discuss the challenges you encountered.
4. Develop a simple application scenario, or reuse an existing application, that must run on at least three hosts and satisfy at least three quality-of-service (QoS) dimensions. Model the application's architecture in xADL. Define formally each QoS dimension. Your objective is to determine the optimal deployment of your architecture. What system parameters did you have to consider? Did you run into a Pareto optimal situation?
5. To help you deal with the preceding problem, select a set of system users and elicit utility functions from them. What issues did you encounter in this process? Are your users readily able to provide the information in the form you need? Why or why not?
6. A software system consisting of  $N$  components is distributed across  $M$  hardware hosts ( $N > M$ ). Given
  - a particular deployment for the software system,
  - the definition of system availability as the ratio of attempted inter-component interactions to completed interactions,
  - the reliability for each network link as the percentage of time the link is "up",
  - the bandwidth for each link,
  - the frequency of component interactions,
  - the size of exchanged data in each interaction,
  - the available memory on each hardware device, and
  - the required memory for each component
 Devise an algorithm that will find the system's deployment that will maximize the system's availability. Discuss the computational complexity of your algorithm. Suggest enhancements that may decrease the algorithm's complexity. Discuss the trade-offs you have to consider in order to effect those enhancements. You may assume that a central view of the system's deployment architecture is available.
7. A swarm of  $M$  mobile robots is collaborating to achieve a common task using  $N$  software components. Unlike the above problem, there is no single location from which the system's deployment architecture (i.e., the view of the system such as that shown in the above figure) may be retrieved. In addition, there are the following two constraints:
  - each robot can be connected at most  $M-2$  other robots; and
  - each robot can "see" only those robots to which it is directly connected.

Devise a decentralized algorithm in which each robot autonomously decides the migration of its local components to improve the system's overall availability. You may not assume that any robot will be able to obtain a global view of the system. Each robot may acquire the relevant local deployment information from robots to which it is directly connected.

8. As discussed in this chapter, a component is typically rendered quiescent during migration. However, other, especially remote components will likely continue sending the migrating component service requests. Those requests will not be serviced immediately, and cannot be simply ignored. Devise and describe at least three solutions for servicing the requests made of a component during migration. Compare and contrast your solutions and discuss their trade-offs.

## 10.7 Further Reading

The general problem of software deployment has been studied extensively. However, a comparatively smaller number of existing techniques have tried to address deployment from a software architecture-based perspective. The most relevant related work is overviewed below.

In the deployment modeling area, the Unified Modeling Language (UML) provides *deployment* diagrams, which enable a static visual representation of a system's deployment. SysML [269] is a modeling language standard for specifying systems engineering artifacts. SysML's *allocation* diagrams allow arbitrary modeling elements to reference one another (e.g., allocation of behavioral elements to structural elements, or software elements to hardware elements). Neither UML nor SysML gives engineers feedback as they create or visualize (possibly inappropriate) deployment models of a system. Some promising approaches in deployment architecture modeling have been built on the previous research in architecture description languages. Two notable examples of ADLs that are capable of modeling a deployment view of a system's architecture are xADL [50, 51] and AADL [73]. In fact, the DeSi deployment modeling and analysis tool discussed in this chapter is built around xADL as its architecture modeling core.

Several existing techniques have attempted to analyze the impact of a system's deployment architecture on its provided quality of service. [15] proposes the use of binary integer programming (BIP) for generating an optimal deployment of a software application over a given network, such that the overall remote communication is minimized. Solving the BIP model is exponentially complex in the number of software components, however, rendering it applicable only to small systems. Coign [126] provides a framework for distributed partitioning of COM applications across the network in a manner that minimizes communication time.

Coign only addresses scenarios involving with two-host client-server applications. Component placement problem (CPP) [152] is a model for describing a distributed system in terms of network and application properties and constraints. This technique only searches for a single valid deployment that satisfies the specified constraints.

A wide variety of technologies exist to support various aspects of the deployment process. Carzaniga et. al. [35] provide an extensive comparison of existing software deployment techniques. They identify three classes of software deployment technologies: Installers, Package Managers, and Application Management Systems. Widely used examples of Installers are Microsoft Windows Installer and InstallShield [134]. Examples of Package Managers are Linux RedHat's RPM, and SUN Solaris's pkg commands. Finally, examples of Application Management Systems are IBM Tivoli Composite Application Manager and OpenView from Hewlett Packard. An Application Management System is tasked with active system monitoring (both hardware and software) and various deployment activities that may need to be performed as a result.

Before it is possible to assess and improve a system's deployment architecture, one may need to study and understand the properties of a deployed system. Typically this is accomplished via system monitoring. Numerous techniques have focused on the problem of remote monitoring of a distributed system. They belong in two categories: (1) techniques that monitor an application at the granularity of software architectural constructs (e.g., components, connectors, their interfaces); and (2) techniques that monitor an application at the granularity of system architectural constructs (e.g., software applications, hardware hosts, network links). Prominent examples of the first category are MonDe [46], GAMMA [218], and COMPAS [198], while the some prominent examples from the second category are JAMM [284] and Remos [65].

Re-deployment, in other words, mobility, is a process of installing, updating, and/or relocating a distributed software system. In a software architecture-based system, these activities fall under the larger category of *dynamic reconfiguration*, which encompasses run-time changes to a software system's architecture via addition and removal of components, connectors, or their interconnections. Oreizy et. al. [214-216] describe several aspects of dynamic reconfiguration, which determine the degree to which change can be reasoned about, specified, implemented, and governed. This work is further discussed in Chapter 14. Garlan et. al. [91] propose a general purpose architecture-based adaptation framework, which monitors the system and leverages ADLs in adapting and achieving architectural conformance. However, this approach models the software architectural aspects of a system, but not those of the hardware platforms. Haas et. al. [108] provide a framework for autonomic service deployment

in networks. The authors of this technique consider the scalability of their autonomic algorithms, which divide the network into partitions and perform a hierarchical deployment of network services. However, their approach is not applicable to application-level deployment. Finally, Software Dock [110] is a system of loosely coupled, cooperating, distributed components. It supports software producers by providing a Release Dock and Field Dock. The Release Dock acts as a repository of software system releases. The Field Dock supports a software consumer by providing an interface to the consumer's resources, configuration, and deployed software systems. The Software Dock employs agents that travel from a Release Dock to a Field Dock in order to perform specific software deployment tasks.

## CHAPTER 11

## 11 Applied Architectures and Styles

The preceding chapters have described the core of software architecture, providing the notations, tools, and techniques to enable the designer to specify an architecture, implement, and deploy it. On the basis of those chapters one should be able to approach any design problem and successfully proceed. Such a simple declaration, however, belies the difficulties that arise when dealing with complex problems. Some problems just do not lend themselves to obvious solutions, or simple, uniform structures. One theme that characterized the chapter on designing architectures was benefiting from the lessons of experience. We continue that theme in this chapter, discussing how a wide variety of important and challenging architectural problems have been solved, thereby enhancing the repertoire of insights and styles that a designer possesses to bring to bear on his own problem.

Our motivation is the recognition that most new applications are complex, and must deal with a range of issues. Notably, many applications must deal with issues that arise from the application being on a computer network, wherein the application interacts with other software systems located remotely. Network-based applications may involve the Web, be focused on parallel computation, or focus on business-to-business interaction. We describe architectural styles for these and other applications.

In this chapter we also use the lens of software architecture to explicate a variety of design notions which are at least in part fundamentally architectural, but which have largely been described in idiosyncratic terms, such as “grid computing” and peer to peer (p2p) applications – terminology belonging to other computer science sub-communities, rather than software engineering. Such description enables a more direct comparison of their merits with alternative approaches to similar problems.

The goals of this chapter are thus to:

- Describe how the concepts from the previous chapters can be used, sometimes in combination, to solve challenging design problems.

- Highlight key issues in emerging application domains which have architectural implications, or where an architectural perspective is essential for system development within that domain.
- Show how emerging architectures, such as p2p, can be characterized and understood through the lens of software architecture.

The sections of this chapter deal first with distribution and network-related issues; the increasingly important topic of decentralized architectures is then considered. The chapter concludes with a section on architectures from a few specific domains.

## Outline of Chapter 11

11 Applied Architectures and Styles
11.1 Distributed and Networked Architectures
11.1.1 Limitations of the Distributed Systems Viewpoint
11.1.2 Architectures for Network-Based Applications
11.1.2.1 The REpresentational State Transfer Style (REST)
11.1.2.2 Commercial Internet-Scale Applications
11.1.3 Decentralized Architectures
11.1.3.1 Shared Resource Computation: the Grid world
11.1.3.2 Peer-to-Peer Styles
11.1.3.3 Business-to-Business: Service-Oriented Architectures and “Web Services”
11.1.4 Summary Notes on Latency and Agency
11.2 Architectures from Specific Domains
11.2.1 Robotics
11.2.2 Wireless Sensor Networks
11.2.3 End Matter
11.2.4 Review Questions
11.2.5 Exercises
11.2.6 Further Reading

### 11.1 Distributed and Networked Architectures

The phrase “distributed application” is used to denote everything from an application which is simply distributed across multiple operating system processes all running on the same physical uniprocessor, to highly integrated applications which run on multiple computers connected by the Internet. Distributed applications have been in general use since at least the late 1970’s when commercial networking technologies began to proliferate, and became increasingly common in the 1980’s with the advent of efficient remote procedure calls and the availability of cheap computing power at the fringes of the network. Consequently we do not pretend to offer anything remotely close to a detailed treatment of such

applications here. A variety of excellent texts are available which treat the subject in depth (see, for example, [69, 273]).

In Chapter 5 we discussed in depth one popular approach to constructing distributed applications, CORBA, as representative of a variety of similar approaches (such as The Open Group's Distributed Computing Environment (DCE) [105]). That presentation omitted consideration of the broader issues associated with distributed applications, hence we begin with that discussion here.

### 11.1.1 Limitations of the Distributed Systems Viewpoint

One of the principal motivations for the development of the CORBA technology, and indeed of much distributed computing technology, was to enable use of the object-oriented development style in a distributed computing context. A particular design choice the designers made was to attempt to provide the illusion of “location transparency”. That is, that a developer should not need to know where a particular object is located in order to interact with that object. (Several other forms of transparency are also supported, such as implementation transparency wherein the developer need not know or be concerned with the choice of programming language that a particular object is implemented in.) If such transparency is provided to the developer all the concerns and issues associated with working across a network can be ignored, for those issues will be “taken care of” by the underlying CORBA support.

Unfortunately a quick look at the details of CORBA's API, i.e. the interface that programmers have to work with, reveals that achieving such transparency has not proved to be fully possible. CORBA has a variety of special mechanisms, visible to the programmer, which reveal the presence of a network underneath, and the possibility of various networking issues impacting the programming model.

The multiple difficulties of attempting to mask the presence of networks and their properties from application developers was recognized early and became canonized by Peter Deustch in his short list “Fallacies of Distributed Computing” [59]. As Deustch and his colleague Gosling say, “Essentially everyone, when they first build a distributed application, makes the following eight assumptions. All prove to be false in the long run and all cause big trouble and painful learning experiences.” The fallacies are, as stated by James Gosling:

- The network is reliable
- Latency is zero
- Bandwidth is infinite
- The network is secure
- Topology doesn't change

#### User Visibility of the Network

- There is one administrator
- Transport cost is zero
- The network is homogeneous

Directly addressing any one of these issues may lead to particular architectural choices and concerns. For instance, if the network is unreliable, then the architecture of a system may need to be dynamically adaptable. The presence of latency (delay in the receipt or delivery of a message) may require applications to be able to proceed based upon locally-created estimated values of messages, based upon the value of previously received messages. Bandwidth limitations, and bandwidth variability, may require inclusion of adaptive strategies to accommodate local conditions. Existence of more than one administrative domain may demand that explicit trust mechanisms be incorporated. Accommodating network heterogeneity may involve imposition of abstraction layers or a focus on interchange standards.

Dealing *explicitly* with these issues that arise due to the presence of networking leads to our consideration of network-based and decentralized architectures. Rather than attempting to be comprehensive in our coverage, however, we select several deep examples that reveal how architectures can be designed to accommodate specific needs and goals.

## 11.2 Architectures for Network-Based Applications

We begin with an extended discussion of the REST style, which was first introduced in Chapter 1. REST was created as part of the effort to take the Web from its earliest form to the robust, pervasive system that we rely upon today. The derivation of REST is instructive, as the interplay between requirements from the application domain (namely, distributed decentralized hypertext) and the constituent parts of the style can be clearly shown.

“Tanenbaum and van Renesse ... make a distinction between distributed systems and network-based systems: a distributed system is one that looks to its users like an ordinary centralized system, but runs on multiple, independent CPUs. In contrast, network-based systems are those capable of operation across a network, but not necessarily in a fashion that is transparent to the user. In some cases it is desirable for the user to be aware of the difference between an action that requires a network request and one that is satisfiable on their local system, particularly when network usage implies an extra transaction cost ....” -- Roy T. Fielding in [75]

### 11.2.1 The REpresentational State Transfer Style (REST)

Chapter 1 of this textbook began with a brief exposition of the REST architectural style, describing how it was used to design the post-1994 World Wide Web (which includes the HTTP/1.1 protocol, the Uniform Resource Identifier specification, the Apache web server, and other elements). The goal of that presentation was to begin to indicate the power of software architecture, showing its impact on one of the world's most widespread technologies. That presentation also indicated how software architecture is not something you can necessarily derive by looking at a piece of source code (e.g. the Apache web server), for the Web's architecture represents a set of design decisions that transcends many independent programs. It is the way those programs must work together that the REST style dictates.

The presentation in Chapter 1 did not describe how the REST style was developed: what motivated its creation and what prior architectural influences were combined to yield this influential style. The presentation below is addressed at these topics. Beyond just understanding the "why" of the Web, the reader should see how selected simple styles can be combined in judicious ways to address a complex, and conflicting, set of needs.

#### Application Drivers

The need for a "next-generation" web arose from the outstanding success of the first generation – and the inability of that first generation's architecture to function adequately in the face of enormous growth in the extent and use of the Web. The characteristics of the Web as an application and the properties of its deployment and use provide the critical context for the development of REST.

The WWW is fundamentally a *distributed hypermedia* application. The conceptual notion is of a vast space of interrelated pieces of information. The navigation of that space is under the control of the user; when presented with one piece of information the user may choose to view another piece, where the reference to that second piece is contained in the first. The information is distributed across the Internet, hence one aspect of the application is that the information selected for viewing – which may be quite large – must be brought across the network to the user's machine for presentation. (Note that some current uses of the web, such as for business-to-business transactions, do not fit this model, and are discussed later under web services.)

Since the information must be brought to the user across the network all the network issues listed in the preceding section are of concern. Latency, for example, may determine user satisfaction with the navigation

experience: actions at the client (i.e. the browser) must be kept fast. As large data sets are transferred it is preferable if some of the information can be presented to the user while the remainder of the data transfer takes place, so that the user is not left waiting. Since the Web is not only a distributed hypermedia application, but a *multi-user* application, provision must also be made for circumstances in which many users request the same information at the same time. The latency intrinsic in the transfer of the information is compounded by potential contention for access to the resource at its source.

The Web is also a heterogeneous, multi-owner application. One goal for the Web was to enable many parties to contribute to the distributed information space by allowing locally-administered information spaces to be linked to the broader community's, and to do so easily. This implies that the information space is not under a single authority – it is a *decentralized* application. The openness of the web implies that uniformity of supporting implementations cannot be assumed, nor can the qualities of those implementations. Moreover the information so linked may not be reliably available. Previously available information may become unavailable, necessitating provision for dealing with broken links.

The heterogeneity of the Web also has a prospective view: various contributors to the information space may identify new types of information to link or new types of processing to perform in response to an information retrieval request. Provision for extension must therefore be made.

Lastly, the matter of scale dominates the concerns. Any proposed architectural style must be capable of maintaining the Web's services in the face of continuing rapid growth in both users and information providers. Keep in mind that REST was developed during a period when the number of web sites was doubling every three to six months! The scale of the application today – in terms of users and sites – is far beyond what was imagined in 1994: 50 million active websites/100 million hostnames.

#### Derivation of REST

The REST style was created to directly address these application needs and design challenges. REST, as a set of design choices, drew from a rich heritage of architectural principles and styles, such as those presented in Chapter 5. Figure 11-1 summarizes the architectural heritage of REST. Key choices in this derivation, explained in detail below, include:

- Layered Separation (a theme in the middle portion of diagram) is used to increase efficiencies, enable independent evolution of elements of the system, and provide robustness;

- Replication (left side of the diagram) is used to address latency and contention by allowing the reuse of information;
- Limited commonality (right side) addresses the competing needs for universally understood operations with extensibility.

Also critical in the derivation was the decision to require requests on the server to be independently serviceable or “context-free”; i.e. the server is able to understand and process any request upon it based solely on the information in the request. This supports scalability and robustness.

Finally, dynamic extension through mobile code addresses independent extensibility. The following paragraphs elaborate these issues and choices. More detailed expositions can be found in [75, 76].

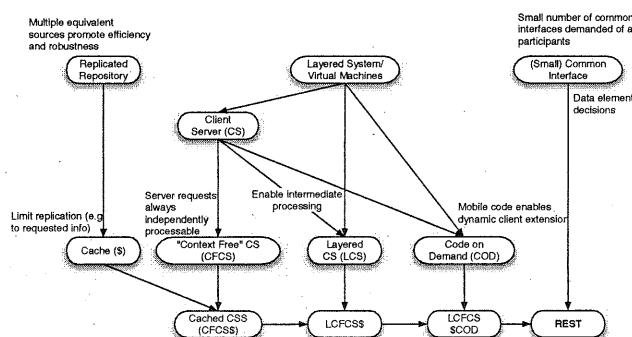


Figure 11-1. Notional derivation of the REST style from simpler styles

### Layered Separation

The core design decision for REST was the use of layered systems. As described in Chapter 5 layered systems can take many forms, including client-server and virtual machines. The separations based upon layering principles can be found several places in REST.

The use of a client-server architecture (CS) was intrinsic to the original Web. Browsers running on a user's machine have responsibility for presentation of information to the user and are the locus of determining the user's next interactions with the information space. Servers have responsibility for maintaining the information that constitutes the Web, and delivering representations of that information to the clients. Software that addresses the user interface can hence evolve independently from the software that must manage large amounts of data and respond to requests from many sources. This separation of responsibilities simplifies both components, and enables their optimization.

The client-server style is then further refined through imposition of the requirement that requests to a server be independently processable; i.e. the server is able to understand and process any request based solely on the information in that one request. This design constraint is often referred to as a “stateless server”, and the corresponding HTTP/1.1 protocol is often referred to as a “stateless protocol”. This terminology is unfortunate, however, as it suggests that the server does not maintain *any* state. The server certainly may maintain state of various kinds: previous client requests may have caused new information to be stored in a database maintained by the server, for instance. Rather, the focus here is that the server does not keep a record of any “session” of interactions with a client. With this requirement the server is free to de-allocate any resources it used in responding to a client's request, including memory, after the request has been handled. In absence of this requirement the server could be obliged to maintain those resources until the client indicated that it would not be issuing any further requests in this “session”. In the diagram we have labeled this specialization of the CS style as “context-free” since a server request can be understood and processed independently of any surrounding context of requests.

Imposition of this requirement on interactions between clients and servers strongly supports scalability, as servers may efficiently manage their own resources – not leaving them tied up in expectation of a “next request”. Moreover all servers with access to the same back-end databases become equal – any one of a number of servers may be used to handle a client request, allowing load sharing among the servers.

The possibility of cheap load balancing is a result of another application of layering in the design of REST. Intermediaries may be imposed in the path of processing a client request. An intermediary (such as a proxy) provides the required interface for a requested service. What happens behind that interface is hidden to the requestor. An intermediary, therefore, may determine which of several equivalent servers can be used to provide the best system performance, and direct calls accordingly. Intermediaries may also perform partial processing of requests, and can do so because all requests are self-contained. Finally, they may address some security concerns, such as enforcing boundaries past which specified information should not be allowed to flow.

### Replication

The replication of information across a set of servers provides the opportunity for increased system performance and robustness. The existence of replication is hidden from clients, of course, as a result of intermediate layers, as described above.

One particular form of replication is caching information. Rather than duplicating information sources irrespective of the particular information actually requested of them, caches may maintain copies of information that has already been requested, or that is anticipated to be requested. Caches may be located near clients (where they may be termed "proxies"), or near servers (where they may be termed "gateways"). The critical feature is that since server requests are always self-contained, as described above, a single cache may be utilized by many different clients. If the cache determines, on the basis of inspecting the request message, that it has the required information, that information may be sent to the requestor without involving any processing on the part of a server. System performance is thus improved since the user obtains the desired information without incurring all the costs that would normally be expected. For this to work, responses from servers must be determined to be cacheable or not. For instance, if a request is for "the current temperature in Denver", the response is not cacheable since the temperature is continually varying. If the request, however, is for "the temperature in Denver at 24:00 on 01/01/2001", that value is cacheable since it is constant.

#### *Limited Commonality*

The parts of a distributed application can be made to work together either by demanding that a common body of code be used for managing all communications, or through imposition of standards governing that communication. In the latter case multiple, independent implementations are possible; communication is enabled because there is agreement upon how to talk. Clearly the use of standards to govern communication is superior to common code in an open, heterogeneous application. Innovation is fostered, local specializations may be supported, different hardware platforms used, and so on. The question, though, is what kind of communication standards should be imposed?

One option is the "feature-rich" style. In this approach every possible type of interaction is anticipated and supported directly in the standard. This approach has the disadvantage that whenever any change to any part of the protocol is required, all implementations must be updated to conform. Another option, the one taken in REST, is essentially two-level. The first level (a) specifies how information is named and represented as meta-data and (b) specifies a very few, key services that every implementation must support. The second level focuses on the packaging of arbitrary data (including any type of request or operation encoded as data), in a standardized form for transmission. This is designed to be efficient for large-grain hypermedia data transfer, thus optimizing for the target application of the Web, but resulting in an interface that is not optimal for other forms of interaction.

#### *Dynamic Extension*

Allowing clients to receive arbitrary data, described by meta-data, in response to a request to a server allows client functionality to be extended dynamically. Data obtained by a client may be, for example, a script or an applet which the client could choose to execute. With such execution the client is able to perform new functions and essentially be customized to that client's user's particular needs. REST thus incorporates the code-on-demand sub-style of mobile code.

#### **Summary**

REST is an exemplar of an architectural style driven by deep understanding of both the particular application domain supported (open network-distributed hypermedia) and the benefits that can be obtained from several simple architectural styles. Constraints from several styles are judiciously combined to yield a coherent architectural approach which is summarized in the box below. The success of the Web is due to this careful engineering<sup>11</sup>.

**Style:** REpresentational State Transfer (REST)

**Summary:** Constrained client-server with focus on data elements communicated.

**Components:** origin server (e.g. Apache httpd, Microsoft IIS); gateway (e.g. Squid, CGI); proxy; user agent (e.g. Safari, Internet Explorer, search bots)

**Connectors:** client-side interface (e.g. libwww); server-side interface (e.g. Apache API); tunnel (e.g. SOCKS, SSL after HTTP CONNECT)

**Data Elements:** resource (the intended conceptual target of a hypertext reference); resource identifier (e.g. URL); representation (e.g. HTML document, JPEG image); representation metadata (e.g. media type, last-modified time); resource metadata (e.g. source link, alternates); control data (e.g. if-modified-since, cache-control)

**Topology:** Multi-client/multi-server with intermediate proxies.

**Constraints imposed:** 6 "REST Principles", or RPs

[RP1] The key abstraction of information is a resource, named by an URL. Any information that can be named can be a resource.

[RP2] The representation of a resource is a sequence of bytes, plus representation metadata to describe those bytes. The particular form of the representation can be negotiated between REST components.

<sup>11</sup> The Web as it exists today in the form of the union of the HTTP/1.1, URI, and other standards, along with various server implementations, should not be equated with REST. Several elements of the Web in current use are at odds with REST; origins of this architectural drift are explored in Fielding's dissertation, as cited earlier.

[RP3] All interactions are context-free: each interaction contains all of the information necessary to understand the request, independent of any requests that may have preceded it.

[RP4] Components perform only a small set of well-defined methods on a resource producing a representation to capture the current or intended state of that resource and transfer that representation between components. These methods are global to the specific architectural instantiation of REST; for instance, all resources exposed via HTTP are expected to support each operation identically.

[RP5] Idempotent operations and representation metadata are encouraged in support of caching and representation reuse.

[RP6] The presence of intermediaries is promoted. Filtering or redirection intermediaries may also use both the metadata and the representations within requests or responses to augment, restrict, or modify requests and responses in a manner that is transparent to both the user agent and the origin server.

**Qualities yielded:** Open, extensible, highly scalable network applications. Reduces network latency in distributed applications while facilitating component implementations that are independent and efficient.

**Rationale:**

**Typical uses:** The World Wide Web (distributed hypermedia)

**Cautions:** Numerous websites and books purport to characterize or exemplify REST principles. The reader should be very cautious, as many sources misrepresent or mischaracterize REST.

**Relations to programming languages or environments:** The code-on-demand and dynamic aspects of the Web favor languages such as JavaScript, Java, Scheme, Ruby, and Python.

The REST style is certainly a powerful tool to use in network-based applications where issues of latency and agency (authority boundaries<sup>12</sup>) are prominent. It is also instructive in guiding architects in the creation of other specialized styles. The tradeoffs made in developing REST, such as how many operations to include in the limited interface specification, highlight that creation of such a style is not straightforward. Nonetheless combination of constraints from a variety of simpler styles can yield a powerful, customized tool.

<sup>12</sup> An agency boundary denotes the set of components operating on behalf of a common (human) authority, with the power to establish agreement within that set [Khare].

## 11.2.2 Commercial Internet-Scale Applications

### Akamai

The REST architecture, as described above, has been successful in enabling the Web to scale through a time period when usage of the Web was growing exponentially. One of the key features of REST that enabled that scaling was caching. While caching may potentially be performed by any component in a REST architecture, a key aspect of REST's support for caching is enabling the presence of intermediaries between a user agent and an origin server, in particular proxies. Proxies can store the results of HTTP GET requests; if the information so stored stays "current" for a time, further requests for that information which pass through that proxy may be satisfied by that proxy, without further routing the request on to the origin server. In dynamic, high-demand situations, however, proxies may not be able to prevent problems. Consider, for example, when a popular sporting event is being covered by a news company, maintaining a record of the event's progress on its website. As the event progresses many thousands of fans may attempt to access the information. Proxies throughout the web will not be of much help because the information is being updated frequently – the contention will be for access to the origin server. These "flash crowd" demands for access to the origin server may induce it to fail, or at least will induce unacceptable latency while each request is processed in turn.

Akamai's solution to the problem is to, in essence, replicate the origin server at many locations throughout the network, and direct a user agent's requests to the "replicant" origin server, called an edge server, closest to that user. This redirection, referred to as mapping, is performed when the Internet address (IP address) for the requested resource (such as "www.example.com/bicycle-race/") is determined by the Internet Domain Name Server (DNS) – one of the first steps in processing an HTTP GET request. Akamai has located many thousands of its edge servers throughout the Internet, such as at the places where Internet Service Providers (ISPs) join their networks to the Internet. One of Akamai's strengths is in the way in which the "closest" edge server is identified. This calculation may involve the results of monitoring the status of parts of the Internet and computing locations whose access will be least impeded by demand elsewhere in the network. The edge servers, of course, will have to access the origin server to update their content, but by directing (and) user agent requests to the edge servers, demand on the origin server is kept manageable.

Viewed architecturally, Akamai further exploits the notion of replicated repositories. REST's separation of resources from representations enables many edge servers to provide representations of the resource located at the origin server. Further, REST's context-free interaction protocol enables

many requests from a single user agent to be satisfied by several different edge servers. Akamai's redirection scheme succeeds because of the strong separations of concerns present in the Internet protocols.

### Google

Google as a company has grown from offering one product – a search engine – to a wide range of applications. Since the search engine and so many of Google's products are so closely tied to the Web one might expect the system architecture(s) to be REST-based. They are not. Google's systems are architecturally interesting, however, because they address matters of scale similar to the Web, but the nature of the applications and the business strategy of the company demands a very different architecture. Google is interesting as well because of the number of different products that share common elements.

The fundamental characteristic of many of Google's applications is that they rest upon the ability to manipulate very large quantities of information. Terabytes of data from the Web and other sources are stored, studied, and manipulated in various ways to yield the company's information products. The company's business strategy has been to support this storage and manipulation using many tens of thousands of commodity hardware platforms. In short, inexpensive PC's running Linux. The key notion is that by supporting effective replication of processing and data storage a fault-tolerant computing platform can be built which is capable of scaling to enormous size. The design choice is to "buy cheap" and plan that failure, of all types, will occur and must be effectively accommodated. The alternative design would be to buy, for example, a high-capacity, high-reliability database system, and replicate it as required. Whether this would be as cost-effective is debatable (it most probably would not), but another key insight from Google's design process is that their applications do not require all the features of a full relational database system. A simpler storage system, offering fewer features, but running atop a highly fault-tolerant platform meets the needs in a cost-effective manner. This system, known as the Google File System, or GFS, is the substrate that manages Google's highly distributed network of storage systems. It is optimized in several ways differently from prior distributed file systems: the files are typically very large (several gigabytes), failure of storage components is expected and handled, files are typically appended to (rather than randomly modified), and consistency rules for managing concurrent access are relaxed.

Running atop GFS are other applications, notable of which is MapReduce. It offers a programming model in which users focus their attention on specifying data selection and reduction operations. The supporting MapReduce implementation is responsible for executing these functions across the huge data sets in the GFS. Critically, the MapReduce library is

responsible for all aspects of parallelizing the operation, so that the thousands of processors available can be effectively brought to bear on the problem without the developer having to deal explicitly with those matters. Once again, the system is designed to gracefully accommodate the expected failure of processors involved in the parallel execution.

The architectural lessons from Google are several:

- Abstraction layers abound: GFS hides details of data distribution and failure, for instance; MapReduce hides the intricacies of parallelizing operations;
- By designing, from the outset, for living with failure of processing, storage, and network elements, a highly robust system can be created;
- Scale is everything: Google's business demands that everything be built with scaling issues in mind;
- By specializing the design to the problem domain, rather than taking the generic "industry standard" approach, high performance and very cost-effective solutions can be developed;
- By developing a general approach (MapReduce) to the data extraction/reduction problem, a highly reusable service was created.

The contrast between the last two points is instructive: one the one hand a *less general* solution strategy was adopted (a specialized file system rather than a general database) and on the other a *general* programming model and implementation was created (abstracting across the needs of many of Google's applications). Both decisions, while superficially at odds, arise from deep knowledge of what Google's applications are – what they demand and what key aspects of commonality are present.

## 11.3 Decentralized Architectures

In the preceding discussion of REST we referred to the World Wide Web as being a distributed, *decentralized*, hypermedia application. Decentralization refers to the multiple authority, or *agency*, domains participating in an application. The sense is that the various parts of an application are owned and controlled by various parties, and those parts communicate over a network (hence decentralization essentially implies *distribution* as well) to achieve the goals of the application. The Web is a good example of this cooperation between independent agencies. The millions of websites around the world are owned and controlled by as many individuals and organizations. By agreeing to the basic standards of the Web, such as HTTP, any user may traverse the web to obtain information, and in so doing may cross many agency boundaries.

Designing decentralized software architectures poses challenges beyond the design of distributed systems. Designing decentralized applications is not, however, a new idea: everyday society is filled with designed decentralized applications. International postal mail is one large-scale example. Individual countries issue their own postage stamps and control local collection and delivery of mail. International post, however, involves cooperation at several levels between the parties involved. For instance, standards govern how mail is addressed, how postage is marked, and agreements are in place to govern the physical routing and handoff of mail. International commerce is an even more extensive and rich example.

Decentralized architectures are created whenever the parties desiring to participate in an application wish to retain autonomous control over aspects of their participation. Website owners, for instance, typically wish to retain the ability to take their sites off-line at arbitrary times, to add new content, or to add new servers. Such autonomy can be the source of many design challenges. Since there is no single authority, there is no guarantee, for example, that a participant in a system will always be participating with the best of intentions. Since decentralized systems are also distributed, coping with the new challenges of multiple agencies comes on top of the challenges of dealing with latency and the other issues of distribution.

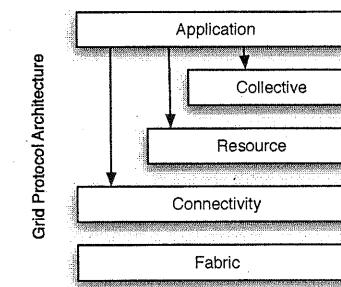
Computer application developers have worked so long in a world where applications were fundamentally centralized in terms of authority (even if under the banner of “distributed systems”) that as we begin to build new applications we have to call those assumptions into question, and adapt to some new realities. This section explores several systems and approaches which have been designed to both exploit the advantages of open, decentralized systems, while mitigating some of the problems encountered. We begin the discussion by briefly discussing grid computing, then focus on several peer-to-peer systems, as they simply and clearly illustrate some of the challenges and design solutions possible. Discussion then turns to “web services”, a design approach targeted to supporting business-to-business interactions.

### 11.3.1 Shared Resource Computation: the Grid world

Grid computing is coordinated resource sharing and computation in a decentralized environment. The notion is to allow, for example, a team of researchers to temporarily bring numerous diverse hardware and software resources to bear on a computational problem. The resources may be under the authority of various owners, but for the time when the grid is “in place” the system behaves as though it is a distributed application under a single authority. The supporting grid technology is designed to make

transparent all the details of managing the diverse and distributed resources. Included in this goal of transparency is management of the details of crossing authority boundaries. A “single sign-on” is thus a particular goal. Grid applications have been used to support visualization of earthquake simulation data, simulate the flow of blood, support physics simulations, and so on.

While many different grid systems have been built, a common architecture for them has been put forth [82], as shown in Figure 11-2. The architecture is layered, with the ability of components within any layer to build upon services provided by any lower layer. The Application layer contains the components that implement the user’s particular system. The Collective layer is responsible for coordinating the use of multiple resources. The Resource layer is responsible for managing the sharing of a single resource. The Connectivity layer is responsible for communication and authentication. The Fabric layer manages the details of the low-level resources which ultimately comprise the grid; the upper layers provide a convenient set of abstractions to this set of resources. The diagram particularly calls out the notion of the application layer calling upon the first three layers below it, but not the Fabric layer. Presumably this is to indicate that management of the lowest-level resources is best left to the grid infrastructure.



**Figure 11-2.**  
Architecture of the  
Grid, according to  
Foster, Kesselman, and  
Tuecke

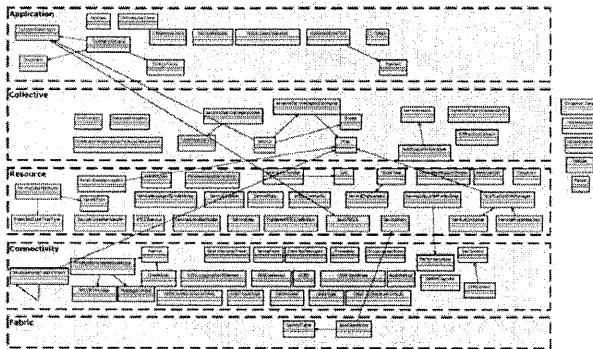
[Adapted from [82]]

Unfortunately the elegance and clean design of this architecture is not fully maintained by several popular and well-known grid technologies. By performing architectural recovery based upon the source code of grid systems, an as-built architecture can be compared to the prescriptive architecture of Figure 11-2. For example, Figure 11-3 portrays the recovered architecture of the Globus grid system, as determined in [185]. In this case, for example, several up-calls in the architecture are present,

violating the layered systems principle. Similar architectural violations have been discovered in other grid technologies as well.

**Figure 11-3.**  
Architecture of Globus Grid technology (recovered).

[From [185]]



### 11.3.2 Peer-to-Peer Styles

Chapter 5 introduced the idea of peer-to-peer architectures. Discussion there centered on the fundamental characteristics of p2p architectures, but did not present many details or rationale for when the style is appropriate. The examples below, Napster, Gnutella, and Skype, add some of this detail.

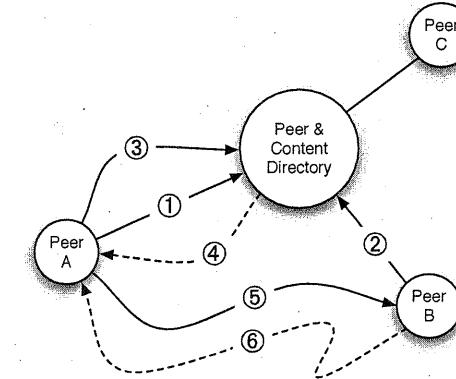
#### Hybrid Client-Server/Peer-to-Peer: Napster

P2p systems became part of the popular technical parlance due in large measure to the popularity of the original Napster system which appeared in 1999. Napster was designed to facilitate the “sharing” of digital recordings in the form of MP3 files. Napster was not, however, a true p2p system. Its design choices, however, are instructive.

Figure 11-4 illustrates the key entities and activities of Napster. Each of the peers shown are independent programs residing on the computers of end users. Operation begins with the various peers registering themselves with the Napster central server. When registering, or later logging in, a peer informs the server of the peer’s Internet address and the music files resident at that peer, which the peer is willing to “share”. The server maintains a record of what music is available, and on which peers. Later, a peer may query the server as to where on the Internet a given song can be obtained. The server responds with available locations; the peer then

chooses one of those locations, makes a call directly to that peer, and downloads the music.

**Figure 11-4.** Notional view of the operation of Napster. In steps 1 and 2, Peers A and B log in with the server. In step 3 Peer A queries the server where it can find Rondo Veneziano’s “Masquerade”. The location of Peer B is returned to A (step 4). In step 5 A asks B for the song, which is then transferred to A (line 6).



Architecturally this system can be seen as a hybrid of client-server and pure p2p. The peers act as clients when registering with the Napster server and querying it. Once a peer knows where to ask for a song, a p2p exchange is initiated; any peer may thus sometimes act as a client (asking others for a song) or as a server (delivering a song it has to another peer in response to a request). Napster chose to use a proprietary protocol for interactions between the peers and the content directory; HTTP was used for fetching the content from a peer. (The choice of a proprietary protocol added no value to the system.)

The architectural cleanliness of this design is also its downfall. If, for example, a highly desired song becomes available, the server will be swamped with requests seeking its location(s). And of course, should the server go down, or be taken down by court order, all peers lose the ability to find other peers.

#### Pure Decentralized P2P: Gnutella

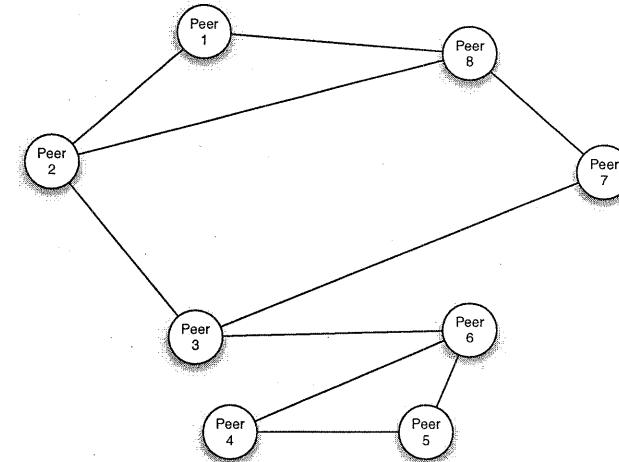
Alleviating the design limitations of Napster was one of the design goals of Gnutella [147]. Gnutella’s earliest version was a pure p2p system; there is no central server – all peers are equal in capability and responsibility. Figure 11-5 helps to illustrate the basic protocol. Similar to Napster, each of the peers is a user running software that implements the Gnutella protocol on an independent computer on the Internet. If Peer 1, for instance, is seeking a particular song (or recipe) to download, he issues

a query to the Gnutella peers on the network that he knows about, peers 2 and 8. Assuming they do not have the song, they pass the query along further, to the peers they know about: each other, and peers 3 and 7. Propagation of the query proceeds to spread throughout the network until either some threshold is exceeded (called the “hop count”), or until a peer is reached that has the desired song. If we assume that Peer 6 has the song, it responds to the peer which asked it (Peer 3), telling 3 that it has song. 3 then relays that information, including the network address of Peer 6, to the peers which requested the information from it. Eventually Peer 1 will obtain the address of Peer 6 and can then initiate a direct request to 6 to download the song. As with Napster, the Gnutella protocol was custom designed, but the direct download of the music was accomplished using an HTTP GET request.

Several issues facing p2p systems are apparent in this example. When a new peer comes on to the network, how does it find any other peers to which its queries can be sent? When a query is issued, how many peers will end up being asked for the requested resource *after* some other peer has already responded and provided the information? Keep in mind that all the peers know only of the requests that they have received, and the requests that they have issued or passed along; they do not have global knowledge. How long should the requesting peer wait to obtain a response? How efficient is the whole process?

Perhaps most interesting, when a peer responds that it has the requested resource, and the requestor downloads it, what assurance does the requestor have that the information downloaded is that which was sought? Experience with Gnutella reveals what might be expected: frequently the majority of responses to a resource request were viruses or other malware, packaged to superficially appear as the requested resource.

These (significant) weaknesses aside, a critical observation of Gnutella is that it is highly robust. Removal of any one peer from the network, or any set of peers, does not diminish the ability of the remaining peers to continue to perform. Removal of a peer may make a specific resource unavailable if that peer was the unique source for that resource, but if a resource was available from several sources it could conceivably still be found and obtained even if many peers were removed from the network.



**Figure 11-5.** Notional interactions between peers using the original Gnutella protocol.

Despite the benefit of being highly robust, the intrinsic limitations of the Gnutella approach have led to the search for improved mechanisms. Recent versions of Gnutella have adopted some of the Napster-ish use of “special peers” for improvement of, e.g., the peer location process.

Napster and Gnutella are interesting mostly for their historical role and for ease in explaining the benefits and limitations of p2p architectures. A mature, commercial use of p2p is found in Skype, which we consider next.

#### Overlaid P2P: Skype

Skype is a popular Internet telephony application built on a p2p architecture. To use Skype a user must download the Skype application from Skype (only). In contrast to Gnutella, there are no open source implementations, and the Skype protocol is proprietary and secret. When the application is run, the user must first register with the Skype login server. Subsequent to that interaction the system operates in a p2p manner.

Figure 11-6 illustrates how the application functions in more detail. The figure shows Peer 1 logging into the Skype server. That server then tells the Skype peer the address of Supernode A which the peer then contacts. When Peer 1 wants to see if any of his buddies are on line, the query goes to the supernode. When the user makes a Skype call (i.e., a voice call over the Internet), the interaction will proceed from the calling peer to the

supernode, and thence either to the receiving peer directly (such as to Peer 2) or to another supernode and then to the receiving peer. If both peers are on public networks, not behind firewalls, then the interaction between the peers may be set up directly, as is shown in the figure between Peer 2 and Peer 3.

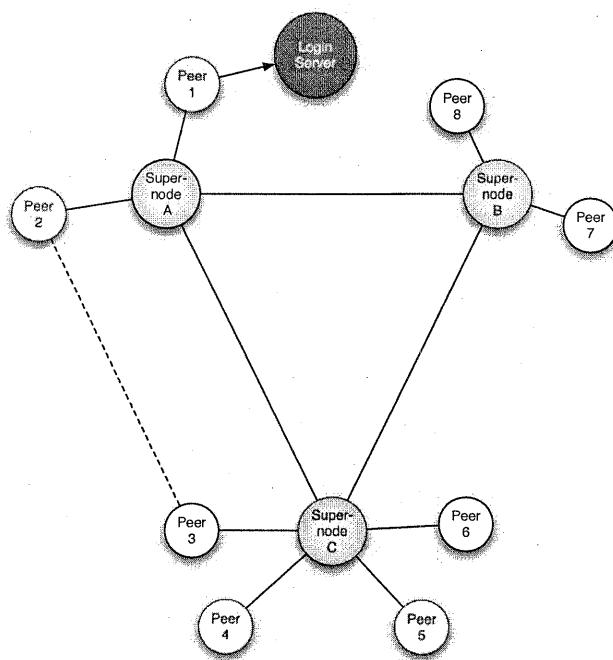


Figure 11-6. Notional instance of the Skype architecture.

Supernodes provide, at least, directory services and call routing. Their locations are chosen based upon network characteristics and the processing capacity of the machine they run on, as well as the load on that machine. While the login server is under the authority of Skype.com, the supernode machines are not. In particular *any* Skype peer has the potential of becoming a supernode. Skype peers get “promoted” to supernode status based upon their history of network and machine performance. The user who downloaded and installed the peer does not have the ability to disallow the peer from becoming a supernode. Note the potential consequences of this for some users. Suppose a machine’s owner installs a Skype peer, and that the owner pays for network

connectivity based upon the amount of traffic that flows in and out of the machine on which the peer is installed. If that peer becomes a supernode then the owner will consequently bear the real cost of routing a potentially large number of calls that he does not participate in and is not even aware of.

Several aspects of this architecture are noteworthy.

- A mixed client-server and peer-to-peer architecture addresses the discovery problem. The network is not flooded with requests in attempts to locate a buddy, such as would happen with the original Gnutella.
- Replication and distribution of the directories, in the form of supernodes, addresses the scalability problem and robustness problem encountered in Napster.
- Promotion of ordinary peers to supernodes based upon network and processing capabilities addresses another aspect of system performance: “not just any peer” is relied upon for important services. Moreover, as many nodes can become supernodes as are dynamically required.
- A proprietary protocol employing encryption provides privacy for calls that are relayed through supernode intermediaries.
- Restriction of participants to clients issued by Skype, and making those clients highly resistant to inspection or modification, prevents malicious clients from entering the network, avoiding the Gnutella problem.

This last point prevents us from too strongly asserting how Skype works. The details provided here have resulted from extensive study of Skype by third-party scientists, citations for which are provided at the end of the chapter. The accompanying sidebar description of Skype is from material provided on the skype.com website.

The following are some of the techniques that Skype employs to deliver state-of-the-art IP-based telephony.

#### Firewall and NAT (Network Address Translation) traversal.

Non-firewalled clients and clients on publicly routable IP addresses are able to help NAT’ed nodes to communicate by routing calls. This allows two clients who otherwise would not be able to communicate to speak with each other. Because the calls are encrypted end-to-end, proxies limit the security or privacy risk.

Likewise, only proxies with available spare resources are chosen so that the performance for these users is not affected.

Several new techniques were also developed in order to avoid end-user

Skype on Skype from  
[www.skype.com](http://www.skype.com)

configuration of gateways and firewalls, whose non-intuitive configuration settings typically prohibit the majority of users from communicating successfully. In short, Skype works behind the majority of firewalls and gateways with no special configuration.

#### Global decentralized user directory.

Most instant message or communication software requires some form of centralized directory for the purposes of establishing a connection between end users in order to associate a static username and identity with an IP number that is likely to change. This change can occur when a user relocates or reconnects to a network with a dynamic IP address. Most Internet-based communication tools track users with a central directory which logs each username and IP number and keeps track of whether users are online or not. Central directories are extremely costly when the user base scales into the millions. By decentralizing this resource-hungry infrastructure, Skype is able to focus all of our resources on developing cutting-edge functionality.

... The Global Index technology is a multi-tiered network where supernodes communicate in such a way that every node in the network has full knowledge of all available users and resources with minimal latency.

#### Intelligent routing.

By using every possible resource, Skype is able to intelligently route encrypted calls through the most effective path possible. Skype even keeps multiple connection paths open and dynamically chooses the one that is best suited at the time. This has the noticeable effect of reducing latency and increasing call quality throughout the network.

### Resource Trading P2P: BitTorrent

BitTorrent is another peer-to-peer application whose architecture has been specialized to meet particular goals. The primary goal is to support the speedy replication of large files on individual peers, upon demand. The distinctive approach of BitTorrent is to attempt to maximize use of all available resources in the network of interested peers to minimize the burden on any one participant, thus promoting scalability.

The problem that BitTorrent solves can be seen by considering what happens in either Napster or Gnutella, as described above, when one peer in the network has a popular item. Any peer who announces availability of a resource (either by registering the resource with the Napster server, or responding to a network query in the case of Gnutella) can quickly become the recipient of a very large number of requests for that resource – possibly more than the machine can support. These “flash crowds” burden

the peer-server possessing the resource and can hence dissuade the server's owner from participating further in the p2p network.

BitTorrent's approach is to distribute parts of a file to many peers and to hence distribute both the processing and networking loads over many parts of the peer network. A peer does not obtain the requested (large) file from a single resource; rather the pieces of the file are obtained from many peers. Moreover the requesting peer does not only download the pieces, but is also responsible for uploading the portions of the file that it has to other interested peers (keep in mind the operating context is one in which many peers are simultaneously interested in obtaining a copy of the file).

Architecturally, BitTorrent has made the following key decisions.

- Responsibility for the discovery of content is outside the scope of BitTorrent. Potential users use other means (Web searches, for example) to locate content on the Web.
- A designated (centralized) machine called the tracker is used to oversee the process by which a file is distributed to an interested set of peers, but the tracker does not perform any of the file transfer. Peers use interaction with this machine to identify the other peers with which they communicate to effect the download.
- Meta-data is associated with the file, and is used throughout the download process. The meta-data describes how the large file is “chunked”, the attributes of those chunks, and the location of the tracker.
- Each peer participating in a file's replication runs a BitTorrent application that determines (a) what piece of the file to download next, and (b) which peer to obtain that piece from. All the participating peers maintain knowledge of which peers have which pieces. The algorithms are designed to achieve the goals of quick distribution through maximizing use of the resources available at all peers. (If a peer is manipulated so that it does not participate in uploading pieces, but only downloading, it is penalized by the other peers through de-prioritization of access to the pieces that it needs.)

As with all well-designed p2p applications, BitTorrent accounts for the possibility of any given peer dropping out of the process at any time.

### 11.3.3 Business-to-Business: Service-Oriented Architectures and “Web Services”

Web services, or service-oriented architectures (SOA) as they are more accurately described, are directed at supporting the interaction of independent businesses on the Internet. The notion is that business A could obtain some processing service b from vendor B, service c from vendor C, and so on. The service that A obtains from C might be based

upon the result obtained from B in a preceding interaction. As a more specific example, a company might obtain bids from multiple travel agencies for a requested travel itinerary, select one of the travel agencies, then have that agency interact directly with subcontractors to contract the various specific services. All these interactions would be supported by SOA mechanisms.

Since independence of the various interacting organizations is fundamental to the SOA vision, service-oriented architectures are conceptually part of the decentralized design space. SOAs must deal with all the network issues of distributed systems, plus the trust, discovery, and dynamism issues present in open, decentralized systems. Indeed, service oriented architectures are the computer-based equivalents of the decentralized systems we see active in ordinary person-to-person commerce: businesses and customers interact with each other in myriad, complex ways. Customers have to find businesses that offer the services they require, must determine if a business proffering a service is trustworthy, engage subcontractors, handle defaults, and so on.

From an architectural perspective, participating organizations on the Internet present a virtual machine layer of services of which users (client programs) may avail themselves. This view is portrayed in Figure 11-7, where a client has an objective (such as obtaining all the reservations, tickets, and travel advances associated with an itinerary) and calls upon various services throughout the Internet to meet this objective. Various of these services may themselves call upon other services on the network to achieve their subgoals. The “virtual machine” of the service-network is rather unlike the virtual machine architectures discussed in Chapter 5, however. The various services (corresponding to functions in a classical virtual machine architecture) are offered by different controlling agencies; they may be implemented in widely varying ways, pose varying risks (e.g. of being impersonated by a malicious agency), may come and go over time, and so on. The challenge, thus, is to provide the necessary support to a client who wishes to use the service-network to achieve its goals. Web services responds to this challenge by offering up a plethora of approaches, standards, and technologies.

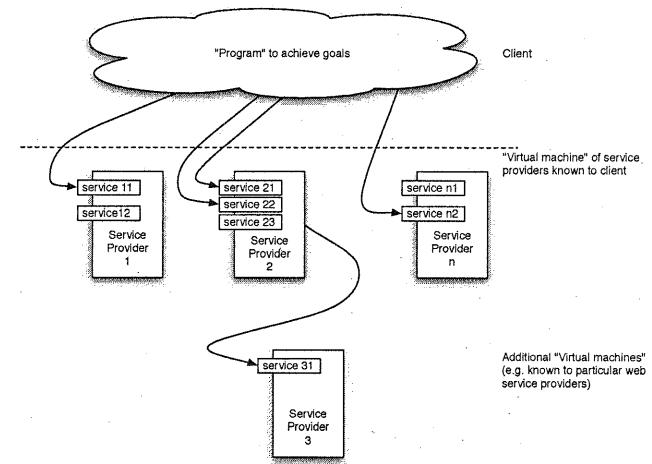
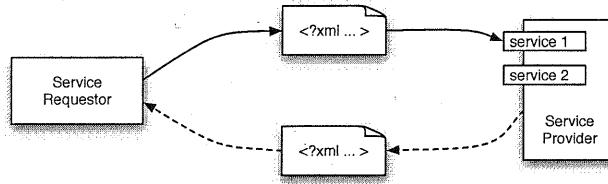


Figure 11-7. Web services as a layered, virtual machine

In essence the core problem is “what architectural model should be built atop the VM of the service network?” The simplest answer given by SOA is asynchronous event notification. The top half of Figure 11-8 illustrates this. The basic model is that a service requestor sends an XML document to a service provider across the network by any of a variety of protocols – anything from email to HTTP. The obligation on both parties is that the XML document is structured so that both understand it. In this simplest model the service provider may take some action upon receiving and reading the document, but there is no obligation for the provider to return anything to the requestor. Naturally there are many situations where the desired interaction is indeed for the provider to return information to the requestor; that is supported too, and is shown in the dotted lines in the bottom half of Figure 11-8. Note that in this second example, the architectural model has shifted from one-way, asynchronous events to an asynchronous request-response model, resembling a remote procedure call or perhaps a distributed object method invocation.

Figure 11-8. Two models of Web Service interaction.



One issue here, of course, is that such interactions do not have the same semantics as a remote procedure call nor the semantics of a distributed object invocation. The presence of agency issues, interaction based upon XML document exchange, and absence of various programming semantics, such as object persistence, are the bases for the differences.

Other architectural models have also been built atop the core service network and document exchange primitives. Notable is the use of publish-subscribe mechanisms for discovery of newly available services or service providers. Other developers have created declarative models for utilizing web services, akin to the interpreter style discussed in Chapter 5. Still others have promoted workflow styles for “programming the Web”. Most – if not all – of the styles discussed in Chapter 5 have been used somewhere in the Web Services world. (Note however that though the web services literature sometimes speaks of a “layered set of protocols” this does not imply a layered architecture, as protocol descriptions often do not correspond to components.)

Despite the simple core model of SOA, in practice there is a great deal of complexity. This complexity arises from attempting to simultaneously satisfy many goals, such as interoperability across heterogeneous platforms, while coping with the difficulties inherent in open, decentralized systems. All this complexity does not necessarily yield an effective approach. For instance, the decision to make service providers announce and support specific services which others can “invoke” – the virtual machines decision – induces a particular kind of fragility and rigidity. Should a service provider ever change the interface to a service then all users of that service must become aware of the change and modify their requests accordingly. This is directly analogous to the problems of programming in a language like Java and having a public method signature be modified – all the code dependent on that interface must change. This SOA design decision was not the only option. Just as not all programs depend on calls to public interfaces, a SOA could have been defined wherein service *requestors* pose descriptions of *computations* that

they would like performed, and leave it to service providers to determine if they are able to perform that computation, and if so, how.

Popular literature regarding web services is replete with acronyms and jargon; some reader caution is in order. The standard which governs how the exchanged XML documents are to be structured and exchanged is SOAP. SOAP used to stand for “Simple Object Access Protocol”, but of course “objects” are not being accessed, so SOAP is now just a name -- but one where all the letters are always capitalized.

Similarly Web Services are sometimes described as being “RPC over HTTP”, when HTTP is used as the transport protocol for SOAP messages. Of course the actions are not the same as for a remote procedure call, so this is inaccurate as well.

Use of the phrase “Web Services” would suggest that Web technology is necessarily involved in Web services – such as a web server. Web servers such as Apache are not necessary to respond to a SOAP message, so “Web Services” is a misnomer too.

The fun starts when you get to the acronyms. They cover standards and approaches for building various “architectural” models on top of a service network, for governing exchange of information in the network, for dealing with the many complexities of a multi-agency, networked world, and so on. The aggregate of the Web Service specifications (e.g. WS-Security, WS-MessageData, WS-Events, WS-Coordination, WS-Policy, WS-Reliability, and many others) is sometimes referred to as WS-\*.

Otherwise known as “the web services death star”. *Caveat emptor*

#### 11.3.4 Summary Notes on Latency and Agency

The preceding sections have covered applications and architectures that have substantial complexity resulting from the need to deal with two primary issues in decentralized systems: latency and agency. Latency has been understood as an issue for a long time, and strategies for dealing with it are well-known. Caching of results, intelligent searching strategies, and judicious use of centralized servers can all play roles in reducing latency.

Agency is a richer issue, and of more recent concern. Agency implies concerns with heterogeneity (e.g. of programming language platforms), unreliability, uncertainty, trust, and security. Effectively coping with all the concerns induced by multiple agencies requires careful thought. The REST style, and styles derived from it, offer proven guidance for dealing

#### Words about Words in Web Services:

with several aspects of both agency and latency. Other issues remain, though, such as trust and security, as discussed in Chapter 13.

## 11.4 Architectures from Specific Domains

This section examines the architectures of applications from a few specific domains. Through this examination we show, by example, how various architectural styles and patterns have been refined and exploited to provide the foundational core of effective solutions. While the architectures are drawn from specific application domains, the techniques used in developing the solution architectures, the analyses that accompanied the design, and even the resulting styles themselves are widely useful, extending beyond the confines of these source domains.

### 11.4.1 Robotics

The field of robotics consists of a class of systems which reveals a great deal of diversity based on differences in the degree of autonomy and mobility the various robotic systems exhibit. Exemplars of this variety are:

- Mobile tele-operated systems, such as bomb disposal robots, where full or partial control of the robot system's movement and actions is in the hands of a human operator who may be located hundreds of miles away.
- Industrial automation systems, such as automotive assembly robotic arms, which autonomously perform pre-defined tasks without the need to move or adjust to their environment, as it is assumed that the environment, by design, conforms to the robot's task and movements.
- Mobile autonomous robots, such as DARPA Grand Challenge vehicles, which are not only responsible for their own autonomous control without human intervention but have to also traverse through and deal with unpredictable environments.

#### Challenges

From an architectural and general software engineering perspective, two factors are primarily responsible for making software development challenging in the robotics domain: the physical platforms and devices comprising the robots and the unpredictable nature of the environments in which they operate.

Robotic platforms are integrations of a large number of sensitive devices prone to malfunctions, such as wireless radio communications and vision sensors, complicating the need to coherently integrate the devices. The software systems operating robotic platforms must be capable of continued operation in the face of diminished hardware capacity and the loss of essential functions. The information provided by hardware devices such as sensors may also exhibit a high degree of unreliability and

intermittent spikes of erroneous sensor readings, necessitating the capacity to not only continue operating but also to compensate seamlessly for such errors.

The second challenging element is the need to operate within environments which can be dynamic and unpredictable. Developing a mobile robot which can traverse unknown terrain through varying weather conditions and with potentially moving obstacles, for example, greatly increases the difficulty of designing its software control systems in a way that can account for and continue operating under conditions not fully predicted during the system's design and development.

Given these challenges and the nature of the domain, several software qualities are of special interest in robotic architectures: robustness, performance, reusability and adaptability. The unreliability of many robotic environments motivates the need for robustness; the often stringent demands of working within a real-time environment (the world in which the robot operates) induces specific performance requirements. The need for reuse of developed software components across a variety of robotic systems is driven by the high cost of developing the high-performance and reliable modules necessary for the domain. Moreover many robotic platforms use the same or very similar hardware components and therefore share a common need for drivers and interfaces for those devices. Finally, adaptability is particularly important given that the same hardware platform can be used with a modified software control system in order to perform a different task with unchanged devices.

#### Robotic Architectures

Robotic architectures have their origins in artificial intelligence techniques for knowledge representation and reasoning. They have been subsequently improved in response to shortcomings in the application of these concepts, as well as general advances in the field. The following sections will present a brief overview of this progression, discussed in the context of specific architectural examples, the trends they embody, and their key architectural decisions and goals.

#### Sense-Plan-Act

Recognizing the inability of building robotic systems using solely artificial intelligence search algorithms over a world model, the *sense-plan-act* (SPA) architecture [204] identifies the necessity of using continuous feedback from the environment of a robot as an explicit input to the planning of actions. SPA architectures contain three coarse-grained components with a unidirectional flow of communication between them, as illustrated in Figure 11-9: The *sense* component is responsible for gathering sensor information from the environment and is the primary interface and driver of a robot's sensors. This sensor information is provided as an input to the *plan* component, which uses this input to

determine which actions the robot should perform, which are then communicated to the *act* component – the interface and driver for the robot's motors and actuators – for execution. To this level of detail the architecture resembles the Sense-Compute-Control (SCC) pattern of Chapter 5. A closer look reveals an important distinction, however.

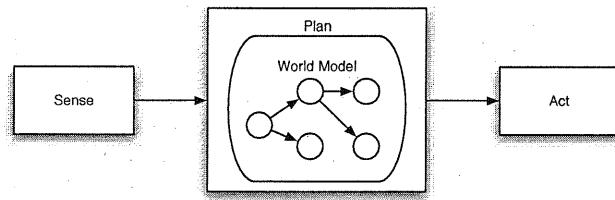


Figure 11-9. An illustration of SPA architectures. The emphasis is on planning actions based on its internal world model sub-architecture.

The *plan* component is the primary driver of robot behavior in SPA architectures. Borrowing from artificial intelligence techniques, planning involves the use of sensory data to reconcile the robot's actual state – as deduced by this sensory data – with an *internal model of the robot's state in the environment*. This internal model is then used in conjunction with a task specification to determine which actions should be performed next by the *act* component in order to complete the robot's intended activity. The internal model is repeatedly updated in response to newly acquired sensory inputs, indicating what progress the robot is making (if any), with the objective of keeping the model consistent with the actual environmental conditions. The SCC pattern, in contrast, does not maintain such a model nor perform sophisticated planning.

From an architectural perspective, the SPA architecture captures an iterative unidirectional data flow between the three components, similar to a pipe and filter architecture, with a sub-architecture for the *plan* component varying and depending on the kind of planning and robot state model used by a specific SPA architecture.

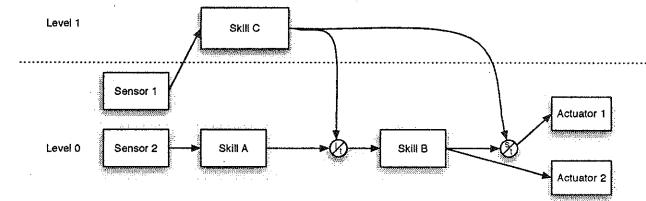
Systems following the SPA architecture suffer from a number of issues primarily relating to performance and scalability. The primary drawback is that sensor information must be integrated – referred to as sensor fusion – and incorporated into the robot's planning models in order for actions to be determined at *each step* of the architecture's iteration: these operations are quite time consuming and normally cannot keep up with the rate of environmental change. The performance of this iterative model-update-and-evaluation does not scale well as robotic system capabilities and goals expand. This poor performance is quite a handicap when the environment

changes at a quick rate or unpredictably, and is the primary driver for the development of alternative robotic architectures.

### Subsumption

Attempting to address the drawbacks of SPA architectures, the Subsumption architecture [32] makes a fundamental architectural decision: the abandonment of complete world models and plans as the central element of robotic systems. While the flow of information originates at sensors and eventually terminates at actuators which effect action (as in SPA architectures), there is no explicit planning step interposed between this flow. Subsumption architectures – as can be seen in Figure 11-10 – are composed of a number of independent components, each encapsulating a specific behavior or robot skill. These components are arranged into successively more complex layers that communicate through two operations: *inhibition* and *suppression*. These operations are used to prevent input to a component or to replace the output of a component respectively. In the figure, output from Skill C may cause the input from Skill A to Skill B to be delayed by time  $t$ ; similarly output from Skill C may override the output of Skill B to Actuator 1 for time  $t$ .

Figure 11-10. An illustration of an example Subsumption architecture, showing the inhibition and suppression operations between levels of components.



The fundamental architectural feature of Subsumption architectures is the modularization of robot behavior and functionality: rather than behavior being represented in a single model, independent components arranged in layers each capture one facet of the overall behavior without a single, overarching representation. Each of these components independently relies on sensory inputs in order to trigger the actions it is supposed to perform, and overall robot behavior emerges from the execution of these actions without a central plan coordinating this behavior. Subsumption architectures, therefore, are more reactive in nature. This characteristic explicitly addresses the performance shortcomings of SPA architectures, and Subsumption architectures garnered popularity for their fast and nimble performance.

Architecturally, Subsumption adopts a component-based approach to the basic data flow between sensors and actuators allowing for data flow

cycles, although the interfaces of these components are simple and capture the value of a single signal. In contrast to SPA, the overall behavior of a Subsumption robot depends on the overall topology of the system and how components are connected rather than a single abstract model.

Subsumption architectures are not without drawbacks, despite their better performance characteristics compared to SPA robots. The fundamental drawback of Subsumption in practice lies in the lack of a coherent architectural plan for layering and consequential support. While the conceptualization of the Subsumption architecture describes the use of layers in order to organize components of different complexities, there is no explicit guidance or support for such layering in the architecture. Components are inserted into the data flow depending on their specific task, without their position necessarily being related to the layer within which they are positioned, and without components belonging to the same layer being inserted in similar manners and positions.

### *Three-Layer*

Following the development of Subsumption, a number of alternatives were developed that attempted to bridge the gap between SPA's plans and Subsumption's reactive nature: these hybrid architectures can be grouped together under the rubric of *three-layer* (3L) architectures, with one of the earliest examples being found in [78]. The widely adopted 3L architectures – illustrated in Figure 11-11 – are characterized by the separation of robot functionality into three layers (the names of which may differ from system to system): the *reactive* layer which quickly reacts to events in the environment with quick action, the *sequencing* layer which is responsible for linking functionalities present in the reactive layer into more complex behaviors, and the *planning* layer which performs slower long-term planning.

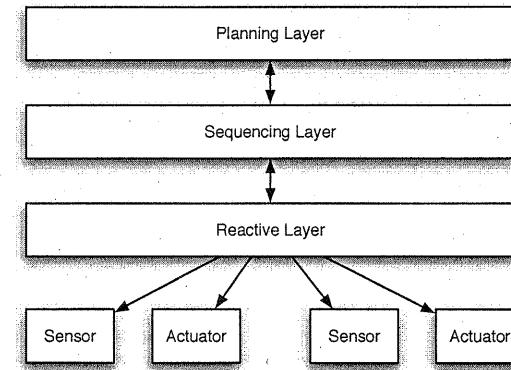


Figure 11-11. An illustration of 3L architectures, showing the relationship between each layer and the basic sensors and actuators.

With the adoption of three separate layers each concerned with a different aspect of a robot's operation, 3L architectures attempt to combine both reactive operation and long-term planning. The planning layer, then, performs tasks in a manner similar to SPA architectures by maintaining long-term state information and evaluating plans for action based on models of the robot's tasks and its environment. The reactive layer – in addition to containing the basic functions and skills of the robot such as grasping an object – captures reactive behavior that must execute quickly and immediately in response to environmental information. The sequencing layer which links the two is responsible for linking reactive layer behaviors together into chains of actions as well as translating high-level directions from the planning layer into these lower-level actions. The majority of 3L architectures adopt some kind of special purpose scripting language for the implementation of the sequencing layer of the architecture. The sequencing layer, then, is often simply a virtual machine which executes programs written in these scripting languages.

From an architectural perspective, 3L is an example of a layered architecture with a bidirectional flow of information and action directives between the layers while using independent components to form each layer. The behavior of 3L architectures is dependent not only on the arrangement of their components, but also on the operation of the internal sub-architecture of the sequencing layer.

One challenge associated with the development of 3L architectures is understanding how to separate functionality into the three layers. This separation is dependent on the robot's specific tasks and goals and there is little architectural guidance to help in this task with the separation largely

depending on the design expertise of the architect. Depending on the tasks the robot is intended to perform, there is also a tendency for one layer to drastically dominate others in importance and complexity, which clouds the hybrid nature of 3L architectures. The interposition of the sequencing layer in the middle of the architecture also results in difficulties when translating the higher-level planning directives into lower-level execution. This translation necessitates the maintenance and reconciliation of the potentially disparate world and behavior models maintained by the planning and sequencing layers, and may cause unnecessary performance overhead.

#### *Reuse-Oriented*

Following the development and widespread use of 3L hybrid architectures, the focus of recent robotic architecture efforts has shifted to the application of modern software engineering technologies to the robotics domain with the primary goal of increasing the level of component reuse and therefore maximizing returns on the time and cost invested in their development. While many of these systems adopt ideas and principles from the previously discussed architectures and exhibit varying degrees of layering and sub-architectures based on planning or task modeling, their primary focus is a clear definition of interfaces and the promotion of reuse.

The primary techniques and technologies these reuse-oriented architectures adopt are explicit object-oriented interface definitions for components and the use of middleware frameworks for the development of components that are reusable across projects. The architecture of the WITAS project [68], for example, adopts CORBA as the mechanism for information interchange and enforces clearly defined interfaces for each component using CORBA IDL, while adopting a hybrid approach that uses a special-purpose *task procedure* specification language sub-architecture for decision-making and planning. In addition to enabling reuse, this approach also enables the distributed operation of robot components for better resource utilization. Another example of this class of systems can be found in the CLARATy architecture [202]: this two-layer architecture adopts a goal-network approach for planning while focusing on defining generic device interfaces clearly identifying the primary functions of a class of devices in a way that is decoupled from the specific device used in any particular instance of a CLARATy architecture. By doing so, different devices of the same type (rangefinders, for example) can be seamlessly integrated into the architecture without the need to re-define this device's interface.

**A look at development frameworks for robotic systems.**

While many robotic systems are designed and built independently, a number of frameworks and tools have been developed to facilitate and

speed the development process. Each of these frameworks is usually targeted toward a specific aspect of robotic development, and includes special support for that purpose. While certainly not a complete survey, this sidebar briefly presents some of the more popular ones.

- Player (<http://playerstage.sourceforge.net>)

The Player open-source project is primarily targeted to Unix-based environments, and provides networked accessible interfaces to a large variety of devices with support for distributed operation of robotic components. The framework also supports integrations with the Stage and Gazebo 3D systems for quickly accessible simulation capabilities.

- Orca (<http://orca-robotics.sourceforge.net>)

Orca is an open-source, cross-platform framework (only the core of the project is supported under Windows) focused on developing component-based robotic systems. The Orca project uses the Ice middleware framework for cross-component communication, and Orca provides libraries which ease the use of the middleware.

- Microsoft Robotics Studio (<http://msdn.microsoft.com/robotics>)

The Microsoft Robotics Studio (MSR) is a free integrated environment for robotic system development. MSR supports a .NET-based service oriented architecture with primary support for the C# and VB.NET languages, and the environment includes simulation support through the PhysX simulation engine.

- Lego Mindstorms (<http://mindstorms.lego.com>)

This package combining both hardware and software has found great popularity, primarily because of its low cost and easy application to educational needs. The Mindstorms package combines a collection of servos and sensors along with a special-purpose operating system and the LabVIEW graphical development environment (developed by National Instruments).

#### 11.4.2 Wireless Sensor Networks

Robotic systems represent a very “active” type of application: the software is tasked with making a physical system perform some set of tasks. Sensor nets are, in a manner of speaking, a largely reactive application: their first task is to monitor the environment and report on its state. Wireless sensor network (WSN) systems are now being used in a variety of domains including medical systems, navigation, industrial automation, and civil engineering for tasks such as monitoring and tracking. These systems enjoy the benefits of low installation cost, inexpensive maintenance, easy reconfiguration, and so on. Nonetheless WSN’s can be very challenging to implement, for they may need to be integrated with legacy wired networks, other embedded devices, and mobile networks that include PDAs and cell-phones for user notification.

The wireless devices themselves are typically highly constrained with respect to power consumption, communication bandwidth and range, and processing capacity. Wireless sensor *systems* impose further constraints with regard to fault-tolerance, performance, availability, and scalability.

As reported in [181], the Bosch Research and Technology Center, in conjunction with researchers at USC, have explored how WSNs should be designed to meet the multitude of challenges present. The architecture-centric design that has emerged for Bosch's applications is interesting for it explicitly combines three separate architectural styles to achieve all the system's goals. The design is sketched in Figure 11-12.

As depicted, MIDAS's reference architecture applies three different architectural styles. The peer-to-peer portion of the architecture is shown in the bottom portion of the diagram. It is responsible for deployment activities, including the exchange of application-level components. The publish-subscribe portion of MIDAS corresponds to the communication backbone responsible for routing and processing of sensor data among the various platforms. The service-oriented portion of MIDAS is depicted at the top of the diagram. These services represent generic, but less frequently used system monitoring and adaptation facilities. These services are distributed among the platforms.

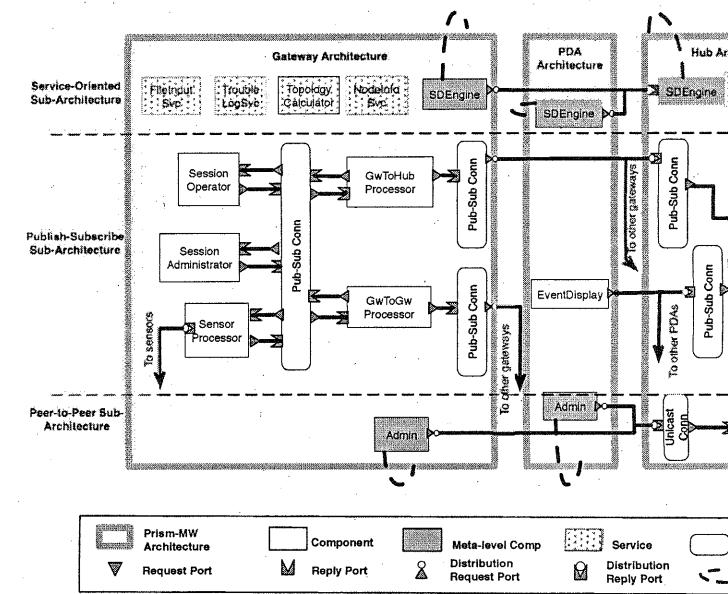


Figure 11-12. The MIDAS Wireless Sensor Network Architecture

Diagram adapted from [181]

## 11.5 End Matter

The central theme of this chapter has been that architectures for complex applications result from deep understanding of the application domain, careful choice of constituent elements and styles based upon experience and their known properties, and hybridization of these elements into a coherent solution. REST is the example *par excellence* of this. The Web would not be the success it is today without this careful architecture.

More than just exemplifying how a complex style arises from the combination of elements from simpler styles, REST illustrates important means for coping with issues that arise due to the presence of network – notably latency and agency. REST thus serves as a model from which solutions to related problems can be derived.

Networking issues – especially latency and agency – have been emphasized in the chapter since an increasingly large proportion of applications are now network based. The discussion of peer-to-peer

systems highlighted concerns with discovery of other peers, search for resources, and risks due to potential performance problems and malicious entities. The particular issues of security and trust will be covered in detail in Chapter 13.

Note that just because an application grows in scope the solution architecture does not necessarily become more complex. Insight into the essence of a problem coupled with effective exploitation of a few simple ideas can yield a highly effective application. This is clearly the case with, e.g., Google, Akamai, and Skype. Great solutions to tough, commercial problems do not just happen: they result from great architectures that reflect experience, choice, and discriminating taste.

**The Business Case**

Development of a great software architecture is a critical step in assuring the long-term financial success of a software product line. Product management and financial difficulties arise when an initial architecture fails to accommodate changes and new demands. Scaling a product to meet new demands in amount of processing is a simple and traditional example. The emergence of the network as the leitmotif of most new applications presents a greater and more subtle challenge than performance, however. In addition to the security risks raised, the network offers the challenges and opportunities of working in an open, dynamic world. The potential is for applications which more quickly adapt to changing circumstances, whether on the individual consumer's side, or in terms of business alliances.

This new landscape presents particular challenges for in-house development of systems. If an organization has traditionally worked only in a closed-shop, LAN-based context, moving to an open network (or even a globally-distributed intranet) it is likely to find the transition rocky. New technologies, and notably new and distinctly different architectures, are required.

## 11.6 Review Questions

1. The eight fallacies of distributed computing, as given in the chapter, are stated as lies. For instance, “The network is reliable.” What are the consequences for a distributed application’s architecture from realizing the network is *not* reliable?
2. What are the consequences for a distributed application’s architecture from the other seven fallacies?
3. What are the three main stylistic elements from which REST was derived?

4. How do “pure” peer-to-peer systems, such as the original Gnutella, discover the presence of resources (like an .mp3 file) in the network? How do hybrid p2p systems improve on that?
5. What are the main styles for robotics architectures, and what problems were observed with the early styles?

## 11.7 Exercises

18. Any two architectural styles can be combined by simply fully encapsulating the use of one style inside of a single component that is present in the usage of the other style. REST however, shows how some styles can be compatibly used together ... at the same level of abstraction. For all pair-wise combinations of the following styles, describe how the styles can be used together at the same level of abstraction, or explain why they cannot.
  - a. Layered/Virtual machines
  - b. Event-based
  - c. Pipe-and-filter
  - d. Rule-based
19. Develop an architecture for the lunar lander video game example that shows the result of (effectively) using two or more architectural styles in combination.
20. Create a diagram like that of Figure 11-1 which indicates the intellectual heritage of the C2 style, as described in Chapter 5.
21. Search on the web and identify other applications (than the web itself) to which REST has been applied.
22. What is the architecture of AOL’s Instant Messenger? How does it compare to the architecture of ICQ’s chat features? How do they compare to the architecture of IRC (Internet Relay Chat)?
23. What are the trust assumptions of the Napster architecture? Develop a modification to the Napster architecture that would decrease the risk of downloading malicious content from another peer.
24. Are service-oriented-architectures peer-to-peer systems? Describe both why this is, and is not, a valid description.
25. Several software architecture styles take inspiration, and sometimes their name, from interactions in real, physical life. “Peer-to-peer” interactions is one example. This relationship can go the other direction too: software architectures can also be used to describe interactions in everyday society. Describe the service architecture of a fast-food restaurant (such as In-an-Out or McDonald’s) using the styles of Chapter 5, in combination as necessary.
26. The Grid Style described in the chapter is very high-level, and described to be broadly descriptive of many grid applications. Identify one actual grid application and describe its architecture. How does that architecture compare to the nominal architecture of Figure 11-2?
27. Koala has been used to develop architectures for consumer electronics, such as televisions. If a distributed media system were to be developed

(with media sources located one place in the network, and various processing and display devices and software located elsewhere in the network), would Koala still be a good choice for describing the architecture? Why or why not? What would be essential in such a situation?

## 11.8 Further Reading

References for further study of distributed architectures and the REST style were provided in the text. Central are Tenenbaum's text on distributed systems [273], and Fielding's dissertation [75] and subsequent journal publication [76].

Google's architecture is becoming increasingly public, with many of its technologies described in papers available at <http://labs.google.com/papers.html>. The Google File System, for example, is explained in [95] and MapReduce is presented in [56].

Further information on Akamai is available in [62]; other resources are available at the company's website.

As the main chapter text mentioned, knowing exactly what is Skype's architecture is somewhat difficult to determine since the client software has been obscured using several sophisticated techniques. The architecture described in the text reflects a forensic analysis. One key publication in this regard is [14], which reflects observation of the Skype client in action. Another project worked at analyzing the obscured client code. Results can be found at <http://recon.cx/en/f/vskype-part1.pdf> and <http://recon.cx/en/f/vskype-part2.pdf>

Good references for web services are somewhat hard to come by. Many publications and web sites are either shallow in their technical presentation, or else focused on only a narrow facet. A good introduction, however, is found in [302]. A technically richer paper is [182].

The architecture of Linux has been recovered and described [26], showing the differences between the application's prescriptive and descriptive architectures. As elsewhere mentioned in this text, the architecture of the Apache web server has also been recovered and described [102, 103]. Both projects are interesting studies in architectural recovery; they are also useful for retrospectively seeing how multiple styles are combined to solve challenging problems.

## CHAPTER 12

# 12 Designing for Non-Functional Properties

Engineering software systems such that they satisfy all of their myriad functional requirements is difficult. As we have seen so far, software architectures can help in that task through effective compositions of well defined components and connectors, which have been verified to adhere to the necessary structural, behavioral, and interaction constraints. While satisfying functional requirements is essential, unfortunately it is not sufficient. Software developers must also provide for non-functional properties (NFPs) of software systems.

**Definition.** A *non-functional property* (NFP) of a software system is a constraint on the manner in which the system implements and delivers its functionality.

Important NFPs of software systems include security, reliability, availability, efficiency, scalability, and fault-tolerance. For example, in the case of the Lunar Lander system discussed throughout this book, the efficiency NFP may be characterized as the constraint that the system must respond to navigation commands within a specific, very short time span; the reliability NFP may be characterized as the constraint that the system may not be in a specified failure state longer than a specific time span.

Software engineering methodology lays stress on doing the "correct things" from the very beginning of the software development process in order to curb development and maintenance costs. In particular, the emergence of the study of software architecture has marked an important trend in software system design—one that in principle allows designers and developers to codify NFPs such as availability, security, and fault-tolerance early on in the architectural models, and maintain their traceability across the system's artifacts and throughout its lifespan.

There are, however, still many domains in which certain critical NFPs have not been explicitly identified or dealt with early in development. This is most frequently evidenced by experiences with web-based systems and desktop operating systems. At least in part developers of these systems

have dealt with issues such as security and dependability as an afterthought. For example, many security patches for Microsoft Windows appear only after a security hole is exposed by a third party. Additionally, these existing systems frequently provide no explicit, active description of the system's architecture to be used as a basis for adding capabilities in support of their dependability. Even if they did, however, it is not always clear how those architectural models would be used. Existing literature is almost completely devoid of the relationship of key architectural elements (software components, connectors, and configurations) to a system's dependability.

An added difficulty is that many NFPs tend to be qualitative rather than quantitative and are often multi-dimensional. Thus it is fundamentally hard to measure an NFP precisely and prove or disprove the extent to which it has been addressed in a given system. One such property is, in fact, dependability. Dependability has become an NFP of prime importance in modern distributed and decentralized systems. In an idealized scenario, a dependable system is one on which the users can completely rely. Clearly, this definition is inherently qualitative and can lend itself to subjective interpretations. Dependability can be described more precisely in terms of its different dimensions: a dependable system should be secure, reliable, available, and robust, and at the same time it should be able to deal with failures and malicious tampering such as denial-of-service attacks. However, even if there were well-defined measures for each of the dimensions, quantifying dependability would still present a challenge. For example, it may be difficult to decide in a general case which system is more dependable: one that is highly reliable but not as secure, or one that is highly secure but less reliable.

Another source of pressures on software architects in ensuring NFPs have stemmed from non-technical issues. Traditionally, NFPs such as security or reliability have taken a back seat to the more lucrative attractions of time-to-market, as well as the pressing concerns of functional requirements. In these scenarios, security has been shoe-horned into a software system, sometimes as an after-thought, while reliability is addressed with often problematic implementation-level solutions. In the case of security, these practices are also complicated by the fact that security is hard to implement, so that malicious individuals have almost always had an advantage over software security practitioners.

While the picture painted above may seem bleak, software architectures can significantly improve the prospects for achieving NFP goals. From the perspective of architectural design, employing good design practices can aid the achievement of these properties, just like poor design practices can harm a system. In this chapter we will provide a set of design guidelines a software architect can follow in pursuing several common NFPs:

- efficiency,
- complexity,
- scalability,
- adaptability, and
- dependability.

The guidelines are just that: guidelines. They are not infallible rules that can be mindlessly applied and yet yield good results. Various caveats and exceptions will be discussed. The job of the architect is to think through the multiple issues and determine an appropriate strategy to pursue.

For each of the above NFPs, we will discuss their impact on a software system's architecture, and, conversely, the role of different architectural elements as well as architectural styles in satisfying the NFP. We will discuss both the characteristics that make an architecture more likely to exhibit a given property and the characteristics that may hamper an architecture's support for an NFP. Whenever appropriate, we will illustrate the discussion with concrete examples from existing architectures and architectural styles.

Note that the above list omits security, an NFP of great, and growing, importance. Because of its importance and significant architectural implications, the entire next chapter is dedicated to that topic.

Outline  
of  
Chapte  
r 12

12. Designing for Non-Functional Properties
12.1 Efficiency
12.1.1 Software Components and Efficiency
12.1.2 Software Connectors and Efficiency
12.1.3 Architectural Configurations and Efficiency
12.2 Complexity
12.2.1 Software Components and Complexity
12.2.2 Software Connectors and Complexity
12.2.3 Architectural Configurations and Complexity
12.3 Scalability and Heterogeneity
12.3.1 Software Components and Scalability
12.3.2 Software Connectors and Scalability
12.3.3 Architectural Configurations and Scalability
12.4 Adaptability
12.4.1 Software Components and Adaptability
12.4.2 Software Connectors and Adaptability
12.4.3 Architectural Configurations and Adaptability
12.5 Dependability
12.5.1 Software Components and Dependability
12.5.2 Software Connectors and Dependability
12.5.3 Architectural Configurations and Dependability
12.6 End Matter

- 12.7 Review Questions
- 12.8 Exercises
- 12.9 Further Reading

A term that has entered software engineering literature relatively recently is *quality-of-service* (QoS). This term is typically associated with networking and distributed systems domains, and has been used somewhat imprecisely within software engineering. For example, it is frequently but incorrectly equated with NFPs. Even though we will not focus on QoS specifically in this book, the term warrants a brief discussion so that the reader can relate it properly to NFPs.

A system's QoS can informally be thought of as the degree to which the system delivers its services such that it satisfies its users' expectations—where the users may be humans or other software. Therefore, QoS encompasses a system's functional as well as its non-functional properties. For example, a system that correctly implements its functionality, but is vulnerable to malicious attacks or fails frequently, would not provide NFPs such as security, reliability, or robustness; it also would not provide good QoS, for the same reasons. On the other hand, a system that is "unbreakable" would provide the above NFPs (regardless of its functional properties), but may still suffer from poor QoS unless it also provides the functionality its users expect.

## 12.1 Efficiency

**Definition.** *Efficiency* is a quality that reflects a software system's ability to meet its performance requirements while minimizing its usage of the resources in its computing environment. In other words, efficiency is a measure of a system's resource usage *economy*.

Note that this definition does not directly address the issue of system correctness. Instead, it implicitly assumes that the system will function as required. In other words, a system cannot be considered efficient if it implements the wrong functionality.

A common misconception is that software architecture has little to say about efficiency since architecture is a design-time entity while efficiency is a runtime property. This is wrong. Selecting appropriate styles or patterns and instantiating them with appropriate components and connectors will have a direct and critical impact on the system's

performance. While it is difficult to enumerate all of the possible performance requirements and related architectural decisions, we will outline certain general guidelines. The reader should be able to use these guidelines as a starting point for a more complete list that will be amassed over time in the reader's personal arsenal.

### 12.1.1 Software Components and Efficiency

#### Keep components small.

For efficiency, ideally each component should satisfy a single need and serve a single purpose in the system. This helps one to avoid employing components the majority of whose services are unused.

The reader should note this guideline can directly impact a component's reusability: many off-the-shelf components are very large and by design include significant functionality that may not be needed in a particular system. Put another way, constructing reusable components can be an impediment to constructing efficient systems.

As with all the guidelines introduced in this chapter, this one should be applied with appropriate caution. Clearly, there will exist off-the-shelf components whose memory footprint and/or runtime performance have been optimized over time; such components will likely outperform one-of-a-kind components built from scratch. Another, quite common exception is a direct by-product of caching: caching data locally for later use can result in components with larger memory footprints, but can also result in faster systems.

#### Keep component interfaces simple and compact.

A software component is accessed only via its public interface. The interface should expose only those component services that are intended to be visible from the outside. Similarly, in general, a component should never expose its internal state other than via the operations intended to modify that state.

If a component's interface is cumbersome, generalized for a broad set of usage scenarios, or geared to a broad class of potential clients, the component's efficiency may be compromised. For example, the component may require different types of adaptors or wrappers to specialize it for use in specific contexts. Alternatively, the component may internally convert the parameters to or from a lowest common denominator form.

Conversely, an interface “stripped to its bare bones” can also negatively impact the efficiency of a component. An example is a Unix pipe-and-filter based system, in which the components (filters) rely on untyped ASCII data streams to maximize their reusability. However, this may require one to constantly convert such streams to typed data for more advanced processing, and for improving system reliability as will be further discussed below.

Note that insisting on compact interfaces for the sake of efficiency may negatively impact other desirable properties of the component, such as its reusability, support for heterogeneity, and even scalability. This will be discussed in the context of the next guideline, and will be revisited later in the chapter.

#### **Allow multiple interfaces to the same functionality.**

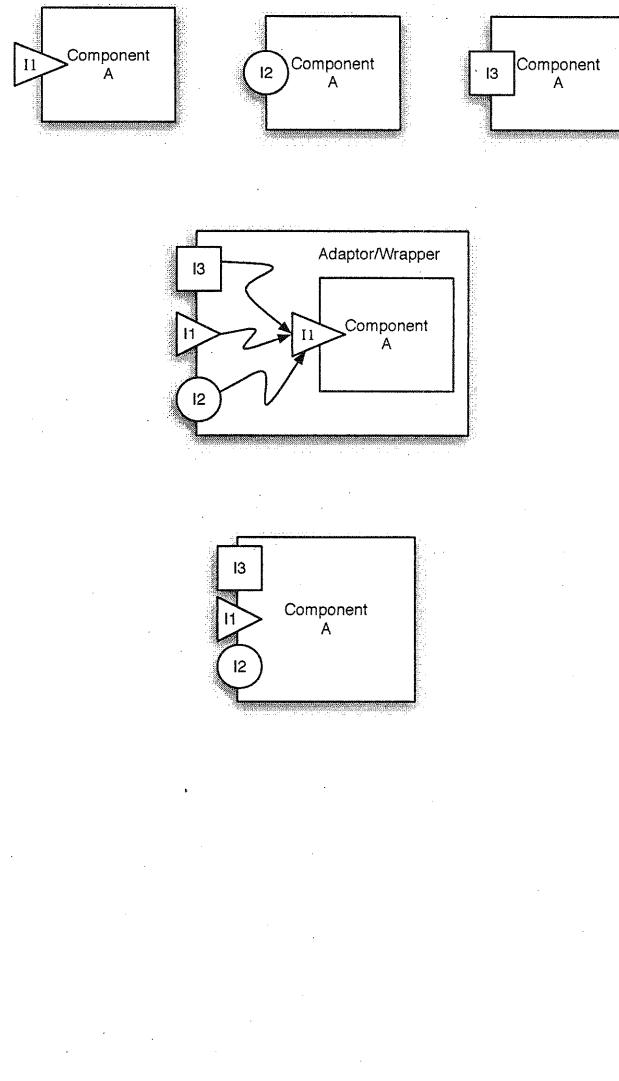
Software components are typically built to be usable in multiple runtime contexts. Even within a single system, they may need to provide services to multiple client components executing on different platforms, implemented in different programming languages, or encoding their data using different standards. They may also need to enforce, for example, different protocols of interaction, transaction support, or persistency rules, as required by the different clients.

In such situations, architects may choose to provide the needed services via multiple components which essentially replicate each other’s functionality. Clearly, that would hurt the system’s efficiency (unless the system is distributed in such a manner that a physically closer copy of the component in question is provided with the appropriate locally needed interface).

Another option is to wrap the component using an adaptor connector that performs all of the needed data conversions. Such a solution is more flexible as the component itself remains unchanged and maintains its memory footprint and runtime performance properties. At the same time, the adaptor will likely introduce some amount of runtime overhead.

Since the adaptor-based approach may result in a narrowly-applicable component, a third option is to construct the component such that it *natively* exports multiple interfaces to its functionality. This solution will likely be more efficient than both of the above options. At the same time, as discussed above, this solution carries the danger that the component will be bloated in situations where only one of its interfaces may be used. The three options are illustrated in Figure 12-1.

**Figure 12-1.** Alternatives for allowing a component to export multiple interfaces to the same functionality: multiple copies of the same component exporting different interfaces (top); a wrapper exporting the different interfaces (middle); the component itself exporting the three interfaces (bottom).



### Separate processing components from data.

Modeling data separately from processing has several potential efficiency benefits. First, it allows the data's internal representation to be fine-tuned or altered, based on local design objectives and without affecting the processing components. Similarly, this allows processing algorithms to be optimized without affecting the data representation, which may be used by multiple components in the system. Separating processing from data also allows architects to ensure, in the architecture, that the appropriate data is at the disposal of the appropriate processing components, thus aiding system correctness arguments.

### Separate data from meta-data.

In many distributed, heterogeneous, data-intensive systems, system data is frequently separated from the meta-data. Meta-data is "the data about the data". In other words, in such systems it may be unclear *a priori* how the data is structured and intended to be used. The data may, for example, arrive at run-time in unpredictable forms. Meta-data can be used as a way of describing the data so that the processing components can discover at runtime how to process the data. Meta-data is heavily used to describe web content elements and the content of email messages.

Separating data from meta-data makes the data smaller, reducing the system's runtime memory footprint: every time a data packet is sent from one processing component to another, it may not need to be accompanied with header information fully describing that data. Thus, if a component already is hard-wired to process data of a particular type, it may do so directly.

On the other hand, keeping the meta-data around and using it to interpret every data packet will, over time, induce a runtime performance penalty in the general case.

## 12.1.2 Software Connectors and Efficiency

### Carefully select connectors.

As argued in Chapter 5, software connectors are first-class entities in a software architecture. They encapsulate all of the interaction facilities in a system. Especially in large, complex, and distributed software systems, the interactions among the system components become the determinants of key system properties, including efficiency. Careful selection of connectors is thus critical.

While many different types of connectors may provide the minimum level of service required by a given set of components in a system, some

connectors will be a better fit than others, and thus may improve system efficiency. For example, the architect may select a message broadcasting connector, such as the connectors in the C2-style Lunar Lander architecture from Chapter 4, because that connector has been used in a number of systems, can accommodate varying numbers of interacting components (that is, its cardinality is N), and has proven to be highly dependable. However, if the particular context in which the connector is to be used involves only a pair of interacting components, then a more specialized, though less flexible, point-to-point connector (with cardinality 2) will likely be a more efficient choice.

Similarly, if the system under construction is safety-critical and has hard-real-time computing or data delivery requirements, a starting point for the architect would likely be synchronous connectors with exactly-once data delivery semantics. On the other hand, if the system being constructed is a weather satellite ground station, a data stream connector with at-most-once data delivery semantics may be a much better choice. It is highly unlikely that a loss of weather data packets over a short time span – even a few minutes – will severely impact the system or its users.

### Use broadcast connectors with caution.

As mentioned above, a system may be more flexible if the connectors used in it are capable of broadcasting data to multiple interested components. For example, new components can attach to such a connector seamlessly and begin observing the relayed information. However, that flexibility can come at the expense of other system properties, such as security and efficiency.

It is possible that a single interaction may involve multiple components, and the temptation may thus be to rely on broadcast. The downside occurs if some of the components receiving the information do not actually need it. In that case the system's performance is impacted, not only because data is unnecessarily routed through the system, but also because the recipient components have to devote some of their processing time to establish whether the data is relevant to them.

An alternative to broadcast connectors is multi-cast connectors, which maintain an explicit mapping between interacting components. Another possibility is to rely on a publish-subscribe mechanism to establish such a mapping during runtime.

### Make use of asynchronous interaction whenever possible.

In a highly distributed and possibly decentralized setting, it may be difficult for multiple components to synchronize their processing such that their interactions take place at times that are ideal for all of the involved

components. If this does not happen and the connectors servicing the components only support synchronous interaction, then, in essence, the slowest component will drag down the performance of the entire system, and may result in multiple components having to wait idly until an interaction can be completed.

In such situations, asynchronous interaction is preferable, where a component is able to initiate the interaction via the connector and then continue with its processing until a later time when it receives a response. Likewise, each invoked component will respond to the incoming service requests as its availability and processing load allow; after it services the request, the component will send its reply to the connector and immediately be able to continue with its processing.

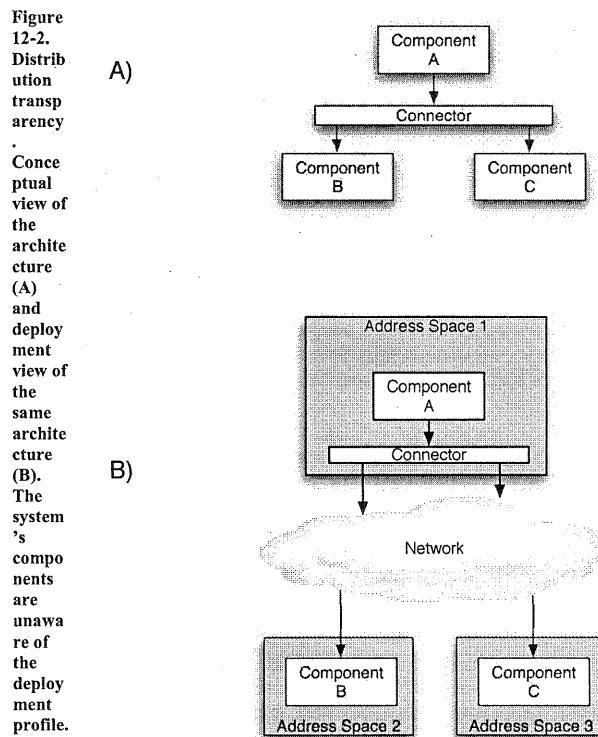
Note that this will not always be possible (single-threaded systems being the simplest example), nor does it come without a performance cost. If the interaction among a set of components is asynchronous, it will be the connector's responsibility to ensure that the service requests and replies are properly associated with one another.<sup>13</sup> This means that the connector will have to do additional processing to maintain many such mappings, determine the ordering of requests and replies, as well as their destinations. Furthermore, the nature of a given component, or of a given request, may be such that the component has to suspend its processing and wait for a response, in which case the benefit of employing an asynchronous connector will be lost.

#### Use location transparency judiciously.

Location transparency, also referred to as distribution transparency, shields a distributed system's components from the details of their deployment. In principle, this allows components to be designed as if all of their interactions are local, that is, that they are co-located on one host with all of the components with which they need to interact. In turn, this allows easy system adaptation, enabling redeployment of some of the components across hosts without affecting the remaining components: it is the task of the systems' connectors to ensure this transparency. An illustration is provided in Figure 12-2.

<sup>13</sup> In many systems this may be accomplished by having components themselves maintain the correspondence between requests and replies, e.g., by associating and exchanging special identifiers ("tokens") with the request and reply messages. While such solutions may work in practice, this association is ultimately an interaction issue, and as such belongs in the connector.

In practice, however, complete location transparency is difficult to achieve. Remote interactions, for example, are many times slower than local interactions. By some measurements they may be slower by a factor of 40 or more. Thus both the interacting components and their users may quickly notice the difference. This means that any distributed system with specific performance requirements *and* the goal of location transparency may have to assume the worst case scenario – that each component is located on a separate host. A preferred alternative is to clearly distinguish remote from local connectors. This may impact the system's adaptability but ensure appropriate performance.



transp  
arent.  
If the  
same  
connec  
tors  
are  
used  
for  
local  
and  
distrib  
uted  
scenari  
os, the  
system  
's  
efficien  
cy will  
likely  
be  
compr  
omised

### 12.1.3 Architectural Configurations and Efficiency

#### Keep frequently interacting components close.

The number of indirections through which two or more components communicate will hamper that interaction's efficiency. This is especially the case for systems with real-time performance requirements.

Architectural styles or configurations that place many points of indirection between such components will be a poor fit. For example, if a component A naturally fits two or more layers above component B in a layered architecture, yet the two components need to interact frequently in a short time frame, a strictly layered architecture is not a good choice for the system: every interaction will need to be forwarded by the intermediate layers.

An example of a layered architecture in which the distance between interacting layers proves to be a problem is that of the mobile robot system discussed by Shaw and Garlan [259], and depicted in Figure 12-3. The *Robot Control* component observes the environment and invokes the *Sensor Interpretation* component in response to events of interest. In turn, the *Sensor Interpretation* component may need to invoke the component (that is, layer) above it, *Sensor Integration*, for a more meaningful, non-local interpretation of the sensed events. Likewise, the *Sensor Integration* component may require the help of the component above it, and so on, until eventually the highest-level component, *Supervisor*, is reached. Once

a component in a given layer is capable of servicing the request it received, it returns the results to the component immediately below it; this sequence continues until the *Robot Control* component receives the necessary information to respond to the sensed event.

In this architecture, it is possible that a request from *Robot Control* must be propagated to as many as seven other components, and returned via them, before it is serviced. For example, if a given class of events from *Robot Control* pertains to the robot's *Navigation*, these events are still propagated, and the responses to them returned, via the three intermediate components. Clearly, this is not an efficient solution. Shaw and Garlan recognize this and discuss several alternative architectures for the system.

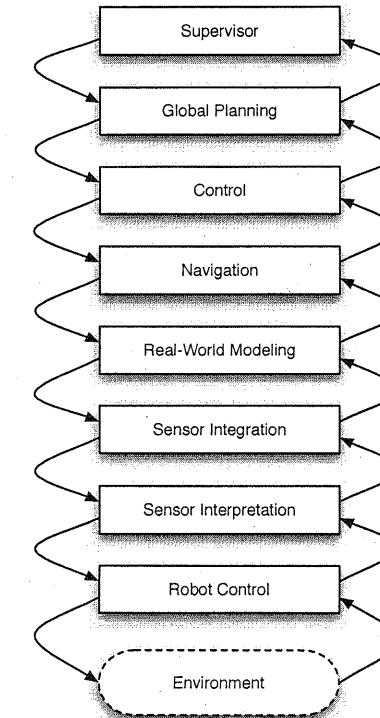


Figure 12-3. A layered architecture for a mobile robot system in which the strict layering may induce performance penalties.

A common way of keeping frequently interacting components close is to cache, hoard, or pre-fetch data needed for their interaction. All three of these techniques try to anticipate the remote information that will be needed by a given component, and try to deliver that information during a convenient time, that is, when the impact on the system's overall performance will be minimal, *before* the information is actually needed. This is one way of mimicking location transparency. Caching, hoarding, and pre-fetching are a part of a software connector's duties. Note that such advanced facilities will invariably add to a connector's complexity, which is further discussed below.

#### **Carefully select and place connectors in the architecture.**

Any large system is likely to comprise components with heterogeneous interaction requirements. As discussed in the Chapter 5, it is possible to create large connectors that are capable of servicing multiple components in different ways simultaneously. Multiple such connectors could then be used in the system. However, each connector would support a superset of the needed interaction capabilities, meaning that, in the average case, many of the connector's features would remain unused, yet still consume resources. Furthermore, it will be difficult to optimize the larger, general-purpose connectors.

For this reason, it may be preferable for an architect to choose multiple connectors, each geared to the given subset of components' specific interaction needs, as opposed to fewer but larger connectors that can service more components in the system and their multiple needs. An obvious example is the procedure call connector. Procedure calls are simple and efficient. While, by themselves, they may be unable to provide more advanced interaction facilities, such as asynchronous invocation, they are able to satisfy a majority of today's systems' needs, even in distributed settings. The higher-order connector facilities can of course still be selected and added to the system, but only if and when they are needed.

Likewise, if a given software component has multiple performance requirements, several options are at the architect's disposal. If the component exports multiple interfaces he can employ multiple connectors to service the component, one per interface type. Alternatively, the architect can try to separate the multi-faceted component into multiple separate components.

#### **Consider the efficiency impact of selected architectural styles and patterns.**

Some styles are not a good match for certain types of problem. For example:

- asynchronous interactions, such as those in publish-subscribe systems, cannot be used effectively in systems with real-time requirements;
- large repository-based systems, such as those adhering to the blackboard architectural styles, may make it difficult to satisfy stringent memory constraints;
- systems that are required to process continuous data streams can be designed using event-based architectures, but transforming a stream into discrete events and possibly recomposing the stream after the transfer carries a computational penalty;
- if data needs to be delivered to its user incrementally, a batch-sequential system will be a poor fit. Similarly, a pipe-and-filter system may be as well, unless the employed variant of the pipe-and-filter style supports incremental data delivery.

Additional examples abound.

An analogous argument holds for architectural patterns. For example, the Model-View-Controller pattern may work well in a centralized setting, but it may not be a good fit for highly distributed and decentralized environments because of the frequent tight interaction between the components.

The reader should also note that, while adaptability in certain cases – such as supporting location transparency – may harm a system's efficiency, in other cases system adaptation can be used as a tool to address performance requirements. For example, a style that supports redeployment in a distributed architecture may be able to support certain performance requirements more effectively.

## **12.2 Complexity**

Software complexity can be thought of from different perspectives, and thus defined in different ways. For example, the IEEE definition of complexity [131] is as follows.

**Definition.** *Complexity* is the degree to which a software system or one of its components has a design or implementation that is difficult to understand and verify.

This definition implies that complexity is partial to the specific perspectives of system understanding and verification. The definition does not say how complexity may be manifested in a software system, or how it would impact other objectives, such as satisfying performance requirements. Perhaps worst of all, the determination of the degree to

which a system is complex depends on the particular individual who is asked how “difficult to understand” the system is.

In order to understand the impact of software architecture on complexity the traits of the system itself must be taken into account. A different and somewhat more useful definition follows:

**Definition.** *Complexity* is a software system’s property that is proportional to the size of the system, the number of its constituent elements, the size and internal structure of each element, and the number and nature of the elements’ interdependencies.

In order to make this definition more precise, we would also need to define “size”, “internal structure” and “nature of interdependencies”. At the same time, the reader should have an intuitive understanding of these terms from introductory programming classes. For example, size of a software system can be measured in terms of source lines of code, number of modules, or number of packages. The reader should also be familiar with an element’s internal structure from the discussions of architectural models, and with different types of module interdependencies from the discussion of software connectors in Chapter 4.

There are several observations that emerge from the second definition of complexity and that agree with our general intuitions about software systems. These observations will help us discuss the architectural implications of complexity and formulate some guidelines to help reduce or mitigate its presence.

### 12.2.1 Software Components and Complexity

#### Separate concerns into different components.

Conventional software engineering wisdom suggests that each of the various types of tasks performed by a system should be supported by a different component or set of components. This guideline may be obvious to any software engineer, for it stems from the application of the fundamental software development principles of abstraction, modularity, separation of concerns, and isolation of change. At the same time, this guideline needs to be clarified with respect to a related, perhaps obvious, observation: all other things being equal, a software system with a greater number of components is more complex than a system with a smaller number of components.

At first blush, this would suggest that architects should strive to minimize the number of components in their system. In other words, architects should try to co-locate multiple concerns in a single component in order to

reduce the number of components. In fact, the guideline (that different system concerns should be separated into different components) and the observation (that larger numbers of components result in added complexity) are not inconsistent. In an architecture, the sheer number of components may not be as relevant to the system’s complexity as the number of component *types*. Components of the same type can be easier to understand and analyze, may be more naturally composable, and can help abstract away the details of their instances. Conversely, a system with relatively fewer instances of components, but which are of many different types, may in fact increase overall complexity.

The notion of types used here is broader than that typically employed in the areas of programming languages or formal methods. For the purpose of this discussion, a component type may refer, for instance, to a similar structure, behavior, application domain, organization that developed the components, or standardized API. In other words, a type in this context refers to any set of component features that may ultimately lessen the effort required to properly aid the encompassing system’s construction, composition, integration, verification, or evolution. For example, a system developed entirely in CORBA may be easier to understand than the same system that is developed using a collection of heterogeneous technologies. The reason is that both systems may be composed of the same number of element instances, but the CORBA system is composed of a smaller number of element types.

The reader should also note that reducing the number of components in a system does not guarantee lower complexity if it results in increasing the complexity of each individual component. In other words, a system with larger constituent components is typically more complex than a system with smaller components. Put a slightly different way, a system with more complex components is itself more complex. Again, this is a relative measure and it will depend on the number of components in question. For example, a small number of complex components, belonging to a small number of component types, need not necessarily result in a complex system.

One final observation, applicable both to components and to connectors, is that, from the architectural perspective, individual components are often “black boxes”. As long as they can be treated as such—that is, as long as the engineers can avoid examining the components’ details when establishing a system’s property of interest—their internal complexity does not matter. In other words, this is the very type of complexity that is abstracted away by good architectural design.

Of course, it is a fair question to ask how realistic it is that engineers will not have to consider a component’s internal details. In fact, while

component-based software development has aided engineers in some significant ways, experience to date suggests that the really insidious problems involve the interplay of multiple components and often require the consideration of both their interactions as well as their internal structure and behavior. This is why an architecture-based approach to software development allows the inclusion of many concerns, including intra-component concerns, in the set of a system's principal design decisions.

#### **Keep only the functionality inside components – not interaction.**

While components in a software system contain application-specific functionality and data, they must also interact with other parts of the system, often in intricate and heterogeneous ways. In most commercial software systems, however, a component is encumbered with at least some of its own interaction responsibilities. The most prevalent examples, of course, are the use of procedure calls and shared memory access.

Components typically support one of these two mechanisms in order to integrate and interact with external components.

While there may be legitimate reasons for coupling computation or data with interaction (for example, in order to improve the component's efficiency in a given system), it ultimately violates the basic software engineering principle of separation of concerns and results in more complex components. Furthermore, a decision to place the interaction facilities inside a component may hamper the component's reusability: the interaction facilities will be integrated into the component, yet they may be a poor fit for future systems. For example, if a component incorporates elements enabling it to communicate synchronously via remote procedure calls, that component will be slated for use in certain distributed settings. On the other hand, such design will actually ultimately harm the efficiency of the component, as well as that of its encompassing systems, if the component needs to be used in an alternative setting in which its interactions need to be asynchronous or local, or both; in such cases, adaptor connectors will need to be used to integrate the component with the rest of the system.

Placing interaction facilities inside a component also violates the principle of separation of concerns from the point of view of the connector: the interaction facilities housed within the component will need to be isolated to make them reusable, optimize them, or improve their reliability over time. This will be further discussed below.

#### **Keep components cohesive.**

This guideline is similar to the "Keep the components small" guideline from Section 12.1.1, and we refer the reader back to that section for the

essence of the argument. At the same time, one reality of software development cannot be avoided: regardless of how principled or clever architectural design decisions are, complex problems frequently require complex solutions. Software architecture can play a role in controlling that complexity, but architecture cannot eliminate the complexity. Therefore, a component may in fact need to be complex if the functionality it provides is complex.

Nevertheless, that complexity will be easier to tackle if the component has a clear focus, that is, if it addresses a specific, well defined need in the system and does not incorporate solutions for multiple, disparate system requirements. One example of components that are not cohesive was discussed in the previous guideline: coupling functionality with interaction inside a component will ultimately increase the component's complexity, and may result in several other undesirable characteristics. Another potential such class of components will be discussed next.

#### **Be aware of the impact of off-the-shelf components on complexity.**

In general, off-the-shelf reuse has many well-documented benefits. Among them are the potential to reduce development effort, time, and cost, and to improve system dependability. At the same time, off-the-shelf components are often very large and complex systems in their own right. They may demand a great deal of careful study to understand them, and intricate techniques for integration with other components.

Therefore, off-the-shelf components may impact a system's complexity in two ways: (1) as a by-product of their own internal complexity and (2) by requiring that complex connectors be used in the system. The first source of complexity can be avoided as long as the component can be treated as a black box. However, as soon as the engineer has to "peek inside" the component, the complexity of the system in question may increase significantly.

The second source of complexity arises from a common misconception in off-the-shelf reuse-based development. That misconception is that clean, well documented APIs will necessarily simplify the integration of a component into a new system. While such APIs are certainly needed to effectively use the component, they can still mask many idiosyncrasies in the way the component is actually intended to be used. For example:

- The API will typically not provide guidance on how the component should be configured in a given environment and initialized for use.

- The API may not give any hints about the assumptions made by the component. For instance, does the component assume that it will control the system's main thread of execution?
- The API may not clearly indicate which operations are synchronous, and which ones asynchronous.
- The order in which operations can be legally invoked may be unclear in the API.
- The component state or mode of operation assumed for invoking a given element of the API may be unclear.
- Any side-effects of operations may be unstated.

The connectors required to integrate off-the-shelf components have to account for such details. They will therefore be a very real source of complexity, and one of which a software architect must be keenly aware.

#### **Insulate processing components from changes in data format.**

Processing components that need access to system data will likely rely on that data being presented in a particular format. Should the data format change—which is possible, even likely in long-lived, distributed, and decentralized systems—the components themselves may need to change. Indeed, it is conceivable that a simple change in the data may affect a large portion of a system. Furthermore, the impact of data changes may not be easily foreseen as many architecture modeling notations do not take into account data access dependencies.

To avoid such undesirable situations, architects should employ techniques to control the complexity of processing-to-data and data-to-data dependencies. One such solution is to use dedicated meta-level components to address data resource discovery and location tracking. Another solution is to make use of explicit adaptor connectors that enable the processing components to rely on the same data “interface”. Finally, as discussed in the case of efficiency above, data should be separated from meta-data, allowing components to dynamically interpret the data they are accessing.

## **12.2 Software Connectors and Complexity**

#### **Treat connectors explicitly.**

The impact of coupling functionality, data, and interaction on a system's complexity has been discussed above, in the guidelines for designing, constructing, and selecting components. One of the key contributions of software development from an explicit architectural perspective is that application-specific functionality and data should be separated from the application-independent interaction. That interaction should be housed in

explicit software connectors. The reader should refer back to the Chapter 5 for the many arguments in favor of treating connectors explicitly and the benefits that accrue thereby.

#### **Keep only interaction facilities inside connectors.**

As already discussed in several places throughout this book, connectors are in charge of the application-independent interaction facilities in a given software system. The task of a connector is to support the communication and coordination needs of two or more components, and to provide the needed conversion and facilitation capabilities to improve that communication and coordination.

Nonetheless, just as the temptation may exist to place advanced interaction facilities inside components, it may be similarly tempting to place application-specific functionality or data inside a connector. There are seldom any good reasons to do this – it will always be possible to add a new component to house any such functionality – and there are many reasons not to do it. Therefore, as a general guideline, making a connector responsible for providing application-specific functionality or data should always be avoided.

#### **Separate interaction concerns into different connectors.**

Interaction concerns in a given system could be simply the general connector roles discussed in Chapter 5, such as separating communication from facilitation. Those concerns could also be more application-specific, such as decoupling the exchange of data between two specific distributed components from the compression of that data to enable more efficient transmission across the network.

The basic argument underlying this guideline is analogous to the one applied to software components in Section 12.2.1. In principle, each connector should have a single, specific, well defined responsibility. This allows for connectors to be updated, even at system runtime. It also allows the architect to clearly assess the components interacting through those connectors, as well as the impact of any modifications of those components. Any issues with the system will be easier to isolate and address as well.

#### **Restrict interactions facilitated by each connector.**

In distributed software systems, interaction will often surpass computation as the dominant factor for determining a given system's key characteristics. For example, the study of battery power consumption in some distributed systems has shown that communication costs typically dwarf computational costs; because of this, a system's computational

energy costs are, in some cases, considered to be nothing more than noise, and thus ignored, in the system's overall energy cost assessment.

Similar arguments can be made about other properties, including efficiency, adaptability, and, in particular, complexity. If a connector unnecessarily involves components in interactions in which they are not interested (e.g., by sending them data), the system's overall complexity will increase. In the best case scenario, the interaction attempt will be ignored. In certain situations, components may be forced to make an explicit effort to ignore the unwanted interaction overtures by the connector, that is, some processing will be expended unnecessarily, in addition to the unneeded data traffic. In the worst case, the components may accidentally engage in the interaction and erroneously affect the system's functionality and state. In such situations, discovering which interaction paths – intended or accidental – caused the system defect may be very difficult.

The simplest rule-of-thumb is to use direct point-to-point interaction whenever possible. Indirect interaction mechanisms, such as event-based or publish-subscribe, are very elegant means for ensuring many properties in distributed systems, such as adaptability, heterogeneity, or decentralization. However, the specific interactions that take place in the system and which may be causing runtime defects can be difficult to track down when such mechanisms are used. Likewise, synchronous interaction lends itself better to determining precisely the interaction paths among the system's components than asynchronous interaction.

Put another way, while certain styles of interaction and system composition have become prevalent in large, distributed, and decentralized software systems, and are direct enablers of several desirable system properties, they tend to negatively impact the system's complexity. It is an engineering tradeoff.

#### **Be aware of the impact of off-the-shelf connectors on complexity.**

Since connectors provide application-independent services, they would appear to be a natural target for attempting reuse. However, there are a number of pitfalls that an engineer should avoid. Most of these are similar to the pitfalls discussed in the analogous guideline applied to components in Section 12.2.1, and the reader is encouraged to revisit that section. A simple example is reusing a connector that possesses far more features and capabilities than a given situation requires.

One additional observation, specific to off-the-shelf connectors, is that it will typically be more difficult to ensure the proper communication paths

in the given system since the engineer will likely have a lower degree of control as compared to custom-built connectors.

### **12.2.3 Architectural Configurations and Complexity**

#### **Eliminate unnecessary dependencies.**

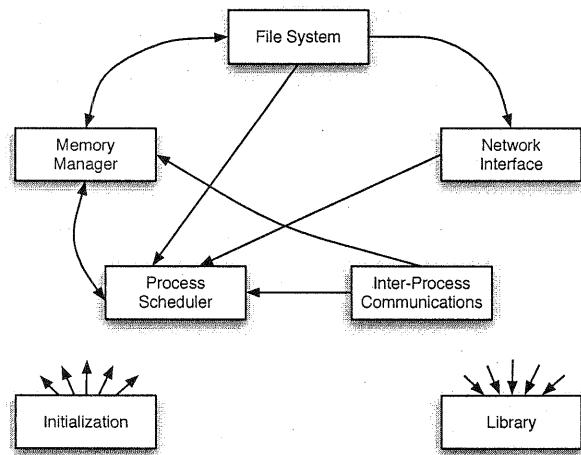
Large software systems are typically more complex than small ones. This means, by extension, that systems with larger software architectures also tend to be more complex. The size of an architecture in this sense can be measured in terms of the size of the architectural model, as indicated for example, by the number of statements or diagram elements in the modeling notation. It can also be measured in terms of the number of constituent components, connectors, and, perhaps most significantly, interaction paths in the architectural configuration.

Most frequently, a system with more interdependencies among its modules is more complex than a system with fewer interdependencies. The reasons are at least two-fold. First, there is a greater number of possible interaction paths in such a system. Second, it is more difficult to control the behavior and predict the properties of such a system, precisely because of the added interaction paths.

Consider, for example, the architecture of the Linux operating system, as studied by Bowman et al. and shown in Figure 12-4 and Figure 12-5. Figure 12-4 shows the “as documented” architecture of Linux, which the authors extracted from the available Linux literature. Figure 12-5 shows the “as implemented” architecture, which the authors extracted from the Linux source code. For the purpose of this discussion, we will treat each identified subsystem as a single component in the architecture; we will further revisit this issue below.

The two diagrams are quite dissimilar: the “as documented” architecture is very clean, with a small number of uni-directional dependencies. On the other hand, the as-implemented architecture depicted in Figure 12-5 is a fully connected graph in which almost all of the dependencies are bi-directional. Any modifications to the bottom architecture will be significantly more difficult to effect correctly because of this added complexity.

**Figure 12-4.** The architecture of the Linux operating system as documented. Adapted from Bowman et al. [26]

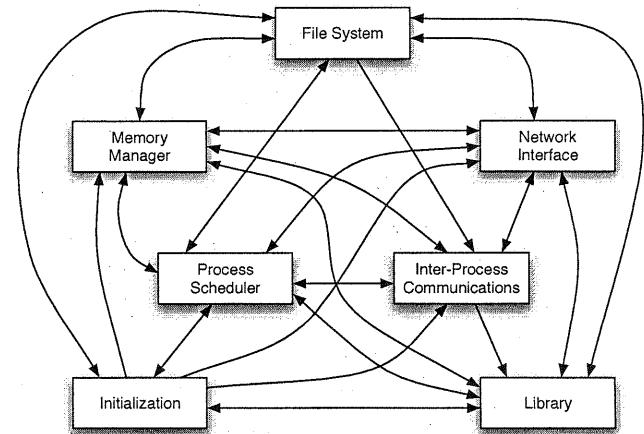


For example, the *Network Interface* component in Figure 12-4 depends only on *Process Scheduler*, and is depended upon by *File System*. On the other hand, in Figure 12-5 the same component both depends and is depended upon nearly every other component in the system; the only exception is the *Initialization* module, with which *Network Interface* has a unidirectional dependency.

The main question in this situation is why are there so many component inter-dependencies, and are they all necessary? Even if they are, an architectural configuration that is revealed via a fully connected graph of components and connectors very likely indicates a poor design.

In such a case, the architect needs to carefully reconsider his design decisions. He may also need to reconsider the selected architectural styles and patterns. While a style or pattern will be unable to eliminate the inherent complexity in a system, a given style or pattern will be appropriate for some classes of problems, but may be inappropriate for others.

**Figure 12-5.** The architecture of the Linux operating system as implemented. Adapted from Bowman et al. [26]



#### Manage all dependencies explicitly.

For illustration, we will continue referring back to the example of Figure 12-4 and Figure 12-5. However, the reader should note that this example is by no means atypical. Cases in which an architecture degrades badly over time abound.

The Linux developers clearly had chosen to call out, and likely rely on, the documented architecture (Figure 12-4) as the correct one. This decision may have been accidental, that is, a product of a long succession of small, undocumented violations to the architecture of which most Linux developers were unaware. On the other hand, the decision may also have been deliberate, as the number of dependencies which an engineer would have to consider—in case a new component had to be added, an existing one modified, or a defect with the system remedied—was much smaller and the architecture easier to justify than would be the case with the architecture in Figure 12-5.

At the same time, the documented architecture clearly omitted a majority of the dependencies. Just because those were hidden from the engineers, their modification tasks would not be made easier. Quite the contrary, engineers may have had to discover these missing dependencies on their own, after they discovered that system adaptations that should have behaved a given way in fact did not work properly. The engineers would in such situations ultimately be forced to study the source code, after

realizing that the documentation is not only incomplete, but also misleading.

It is because of these pitfalls that the real complexity of a system should not, and cannot, be hidden, and that all dependencies should be managed explicitly in the architecture.

#### Use hierarchical (de)composition.

Hierarchical decomposition of a software system's architecture, and hierarchical composition of a system's components, are important tools for managing a given system's complexity. The components of a given conceptual unit are grouped together into a larger, more complex component; that component may also be grouped with other like components into even larger components. Through the use of appropriate interfaces the underlying complexity is masked, allowing the system's architecture at its highest level to be more readily understandable.

For example, the Linux architecture is decomposed into seven key components (that is, Linux subsystems) and their dependencies. Each of these components exports an interface to the rest of the system, and thereby abstracts away the component's internal architecture. This is also frequently the case with off-the-shelf components discussed above, which may be systems in their own right. In principle, a hierarchically (de)composed system allows the architect to isolate the parts of a system that are relevant for a required adaptation.

**Beware of the numbers game**

There is a real danger in reducing guidelines and observations such as found in this chapter to a metric that is then applied blindly. Architects (and their managers) are expected to use their common sense.

For example, to artificially reduce a system's complexity, a simple "solution" may be to make a monolithic system, where all components are and connectors are lumped together into one large module. That would clearly not be a good idea, and would not be the intended implication of these guidelines.

## 12.3 Scalability and Heterogeneity

**Definition.** *Scalability* is the capability of a software system to be adapted to meet new requirements of size and scope.

Even though a system's scalability refers to its ability to be grown or shrunk to meet changes in the size of the problem, traditionally the difficulty faced by software engineers has been in supporting *larger* and thus *more complex* systems. Therefore, we will restrict our discussion to scaling software systems *up*. Software architecture plays a critical role in supporting scalability. There are several dimensions to scalability. Below we will discuss those dimensions and the role software architecture plays in supporting each.

It should be noted that scalability can be achieved in an arbitrary case, but at a potentially exorbitant cost. The objective of this section is to provide guidelines that will allow software architects and engineers to improve a system's scalability without also prohibitively increasing its complexity and deteriorating its performance. In other words, a software system can be said to scale well if its rate of growth is not greater than the corresponding rate of complexity increase.

Two other NFPs deal with system aspects related to scalability: heterogeneity and portability.

**Definition.** *Heterogeneity* is the quality of a software system consisting of multiple disparate constituents or functioning in multiple disparate computing environments.

Since we will often wish to speak of a system easily accommodating heterogeneous elements, that is, accommodating incorporation of disparate components and connectors into its structure, we will also use heterogeneity to refer to an ability:

**Definition.** *Heterogeneity* is a software system's ability to consist of multiple disparate constituents or function in multiple disparate computing environments.

**Definition.** *Portability* is a software system's ability to execute on multiple platforms (hardware or software) with minimal modifications and without significant degradation in functional or non-functional characteristics.

Portability can thus be viewed as a specialization of heterogeneity.

Like scalability, heterogeneity and portability are system properties reflective of the system's ability to accommodate change and difference. They refer to increasing numbers of types of execution environments, in the case of both portability and heterogeneity, as well as types of software elements and users, in the case of heterogeneity.

Heterogeneity can be looked at from two perspectives:

- *Internal heterogeneity* – a system’s ability to accommodate multiple types of components and connectors, possibly written in different programming languages, by different developer teams, and even different organizations; and
- *External heterogeneity* – a system’s ability to adjust to and leverage different hardware platforms, networking protocols, operating systems, middleware infrastructures, and so on. This view of heterogeneity thus encompasses portability.

In the below discussion, for ease of exposition we will focus on scalability as the over-arching property.

### 12.3.1 Software Components and Scalability

A software system’s architecture may need to support the addition of new components. The components may be added as new requirements emerge during the system’s life span. Alternatively, existing components may be replicated to improve system efficiency. In either case, architects should follow some general guidelines to ensure scalability. Again, the reader should remember that these are only guidelines. In general, one should adhere to them whenever possible, yet the reader will probably be familiar with, or will be able to conjure, a software development scenario that would argue against following these guidelines.

In addition to considering the impact of functional component design on scalability, this section will also explicitly consider the impact of the system’s data design. Many systems are highly data-intensive. Presently, that means storing, accessing, distributing, and processing terabytes and even petabytes of data. The World Wide Web can be thought of as such a system. Other examples include scientific applications deployed on a “data grid” (for example, Globus [82] and OODT [186]); such systems are discussed in Chapter 11. In addition to the sheer overall size of the data used by a system, many systems must process that data within specific time constraints. We refer to the amount of data processed in a given amount of time as data *volume* (expressed in bytes per second). Architectural decisions will directly impact a system’s ability to scale up to large data volumes. This section will also identify several heuristics architects should keep in mind when striving for data scalability.

#### **Give each component a single, clearly defined purpose.**

This guideline has analogs in the cases of efficiency and complexity. An architect should avoid placing too much responsibility on any one component. Failing to adhere to this guideline will typically result in large, internally complex components with many dependencies on other components in the system. Such “important” components may also lack

architectural integrity because they encapsulate multiple concerns. They may thus become single points of failure or performance bottlenecks. Scaling up a system that comprises such components will be a challenge because there is an increased chance that any newly added components will also need to rely on the “important” components, further adding to their workload. An example such component is Linux’s *Process Scheduler* from Figure 12-5.

#### **Give each component a simple, understandable interface.**

A component should be easy to identify and understand, use and reuse, deploy and redeploy. A component with a simple interface will have few and clear dependencies on other components in the system. Adding new components will have a minimal impact on such a component. Connectors can be more easily adapted, or new ones introduced, to support interactions with such a component. Finally, such a component will be easier to replicate and distribute across multiple hardware hosts if needed.

#### **Do not burden components with interaction responsibilities.**

As discussed above, this is a common pitfall. Simply put, adding interaction facilities to a component violates the component’s conceptual integrity. Furthermore, it decreases the component’s reusability potential since reuse becomes an all-or-nothing proposition. As discussed previously, it also increases a component’s size and complexity. This has a deleterious impact on scalability. For example, scaling up a system by replicating such a component may become an issue: it may be less clear how that component should interact with the rest of the system since it encapsulates interaction design decisions, which should be public and external to the component.

#### **Avoid unnecessary heterogeneity.**

Component incompatibilities can be overcome, but typically at a price. While it may in some cases significantly reduce development costs and effort, reusing heterogeneous (typically off-the-shelf) components should be approached judiciously. Components that are not carefully tailored to work together can cause *architectural mismatches*. Many examples exist where the needed functionality that was embodied in different components could not be integrated because of discrepancies in the components’ interfaces, assumptions, and constraints.

This, in turn has a direct impact on scalability: a system cannot scale up effectively if adding a single component can fundamentally alter the system’s properties or, worse, break the system. Relying too much on sophisticated connectors is not the answer in such situations either: engineers may manage to integrate the needed functionality, but possibly

at the expense of other properties, such as efficiency, adaptability, or dependability. This is why architectural analysis is an indispensable aid to system integration.

#### Distribute the data sources.

It is possible to imagine a situation in which a system employs a single powerful database that is capable of storing all of its data. Such a decision may be justified for reasons of architectural simplicity or in order to decrease the project's costs. However, if the data needs to be accessed concurrently by many other components in the system, modified, and then stored again, the centralized database may not be able to support the needed data volume, especially if the system needs to grow. In other words, the data source component becomes the system's bottleneck. Furthermore, it becomes a single point of failure.

It is preferable in such situations to distribute the data sources, and possibly task each host with a specific, well defined subset of the data and data consumer components. This enables multiple system components to access the needed data much more efficiently and reliably. The added load on the data storage components that results from adding more data processing (that is, client) components will be distributed more evenly across the system. A significant growth in the size of stored data will be amortized across multiple components. Finally, even if one data source were to fail in such a situation, the remainder of the system could still function in a degraded mode. An example of this approach is BitTorrent [43], which is discussed further in Chapter 11.

#### Replicate data when necessary.

In order to ensure scalable access to system data, a common technique employed in distributed systems is data replication. Replication can help support growing numbers of data consumers; they do not all have to go to the same source. In many distributed systems data replication for local consumption – by a single software component or on a single host – is achieved by caching. Replication can also help the system's fault tolerance: if one of the components containing a copy of the needed data fails, requests for that data can be re-routed to another one of its copies.

Data replication must be approached with appropriate caution, however. Engineers must distinguish between mutable and immutable data. Immutable ("read only") data can typically be replicated with few concerns, save for, perhaps, the security of that data if it is sensitive and access to it needs to be restricted. On the other hand, replicating mutable data requires that all replicas be synchronized. Constant synchronization of distributed copies of the same information can be very expensive

performance-wise, while stale (that is, unsynchronized) data can cause incorrect system behavior and may be unacceptable to the system's users.

### 12.3.2 Software Connectors and Scalability

As new functionality is added to a software system, the system will likely also need to grow in the number of interaction mechanisms, that is, connector types. New connector instances may also be added to improve the system's performance, for example by reducing the load on existing connectors. As in the above case, we can identify some general guidelines that can help to improve a system's scalability in terms of interaction. The reader should, again, keep in mind that these are general guidelines and that it is possible to encounter software development scenarios which may not allow one to adhere to these guidelines.

#### Use explicit connectors.

This guideline may appear obvious by now, but needs to be stressed since the choice to adhere (or not adhere) to it will have significant implications on the given system's scalability. Connectors remove the burden of interaction from components. They are the natural points of scaling in a system. Even when a given connector, such as a remote procedure call, is unable to support the system's scaling up, architects have the opportunity to replace that connector with a more appropriate one, such as an event passing or data caching connector.

System adaptations such as adding new components, extending the system's distribution to new hosts, or increasing the amount of data and the number of data types, can be directly aided by the chosen connectors and, at the same time, should have minimal or no impact on the system's individual components. For example, a component should not need to be aware of the number of other components in the system with which it is interacting.

As discussed in Chapters 4 and 11, software architectures and architectural styles that result in highly scalable systems, such as publish-subscribe or REST, employ explicit, first-class connectors to achieve that scalability.

#### Give each connector a clearly defined responsibility.

If a connector is over-burdened with supporting multiple interaction facets in a given system, large numbers of components, or amounts of data, that connector may not be able to support adequately the system's further growth in size. There are clearly scenarios in which a heavy burden on a connector cannot be avoided. In other situations a connector may be

treated by architects as a software bus that should handle all of the interactions in a system or subsystem. An example is a CORBA ORB.

In such situations, using a larger number of connector instances of the same type is a simple remedy. Each individual connector will thus end up being simpler and responsible for a smaller portion of the overall system's interactions. As such, it will have the potential to support new interactions as needed in the future and hence to aid the system's scalability.

Furthermore, adding new connectors becomes easier because their responsibilities are clearly delineated and component interaction points clearly defined.

Decisions such as the above—to delegate interaction responsibilities to multiple connectors—may be only conceptual, design-time aids, but they will also likely manifest themselves in system implementations.

#### **Choose the simplest connector suited for the task.**

An architect will often have multiple interaction choices at his disposal. For example, as mentioned above, the architect may be able to choose between RPC or a publish-subscribe connector. A decision to go with the latter may be a result of envisioned future system growth, and the impulse may be to go with a far-reaching, more comprehensive solution.

This is not necessarily a wise strategy. Unnecessary complexity usually affects system performance. It is very likely that the system will, in fact, evolve. However, that evolution could be in a direction different than the one anticipated by the architect. Even if the architect turns out to be correct, future adaptations (in this case, future additions of new items such as components, users, points of distribution, and data) should be addressed by introducing the more complex connectors when they are needed. In the meantime, selecting the most appropriate connectors for the system as it currently stands helps to preserve the system's conceptual integrity and will likely speed implementation.

#### **Be aware of differences between direct and indirect dependencies.**

Direct, explicit dependencies between components in a system, such as those captured by synchronous procedure call connectors, can aid architects with controlling the system's complexity and ensuring that its performance requirements are met. However, scaling up such a system may be non-trivial, precisely because the connectors ensure a tight fit among the system's *current* components.

The alternative is to use indirect, implicit dependencies, possibly among multiple components simultaneously, and possibly characterized by asynchronous interaction. In addition to better supporting scalability, such

connectors can also aid system adaptability (further discussed below). Examples seen previously in this book are event broadcasting connectors and shared data access connectors. The advantages of connectors that support loose component coupling come at a cost, however. Such connectors can negatively impact both the system's complexity and performance. For example, how does one discover the sources of system defects when the component interactions are "hidden"? How does one ensure system efficiency when, in principle, multiple components can respond to a given request at arbitrary times and in arbitrary order?

A software architect must be aware of this fundamental trade-off and select connectors judiciously.

#### **Do not place application functionality inside connectors.**

Placing application-specific functionality inside the ostensibly application-independent interaction facilities may be tempting for several reasons. For example, collocating a connector's caching capability with some *in situ* data processing may accrue certain performance gains. However, doing so will violate the separation of concerns principle, and, as discussed above, will result in an increase in the connector's complexity.

Such a decision will also impact the system's scalability. It will likely be more difficult for a connector to service an increasing number of components or route increasing data volumes if the connector is also encumbered with processing responsibilities. Furthermore, the processing done inside the connector may result in additional dependencies with the components, and possible architectural mismatches. Ironically, the ultimate epilogue may well be that the very property used to justify placing application processing inside the connector—improved system efficiency—may end up undermined.

#### **Leverage explicit connectors to support data scalability.**

There are certain types of application-independent data processing that are naturally housed inside a connector. These are techniques for bringing data closer to its consumers and serving it more efficiently or fluidly: buffering, caching, hoarding, and pre-fetching. Such services may need to be tailored to an application. For example, should data be cached after the initial request or pre-fetched in anticipation of future requests; what is the volume of data that needs to be buffered before it is served to a component; under what circumstances should a copy of the data be stored locally?

These services do not alter a system's functionality, hence the system's components should be completely insulated from them. On the other hand, these services can have a significant impact on the system's non-

functional characteristics, in particular, its efficiency and scalability. Therefore, making connectors explicit, first-class entities in the system's architecture is a pre-condition to providing these data scalability services. Recall that this is a major lesson from the REST style (Chapters 1 and 11), which had to enable an unprecedented degree of data scalability in the REST-compliant systems, most notably the World Wide Web.

### 12.3.3 Architectural Configurations and Scalability

#### Avoid system bottlenecks.

If a large and growing number of components depend on services provided by a single other component in a system, that component may eventually become unable to provide its services efficiently or reliably to all of its clients. Similarly, if a large and growing number of components interact through a single connector, at some point that connector may become unable to satisfy the components' interaction needs. In such situations, the overburdened individual components and connectors may have a significant impact on the overall system's performance and may preclude further system growth. In other words, they may become system bottlenecks.

An explicit architectural model can aid with identifying and avoiding bottlenecks. Even a casual glance at the architectural configuration of certain systems can indicate possible bottlenecks. For example, Figure 12-4 suggests that the *Library* component is a potential bottleneck since all other major Linux components invoke it. In order to establish whether *Library* is indeed a bottleneck, additional information is needed: how frequently is it called; what is the latency of servicing requests; are any requests "dropped" because of the component's inability to service them quickly enough; is the performance of other system components significantly impacted by this component's performance?

If the component or connector is established as being a bottleneck in the system, the system may need to be redesigned to eliminate this problem. For example, a replica of the overburdened component may be introduced to service a portion of the requests; likewise, a new connector may be inserted to off-load the original connector by servicing a subset of the interacting components. In distributed systems literature, such techniques are commonly referred to *load balancing*.

#### Make use of parallel processing capabilities.

Certain types of problems lend themselves naturally to processing in multiple parallel threads. Examples are many scientific computing applications. In such cases, the system's scale in the amount of

computation performed or the volume of data processed will depend upon the number of concurrently executing modules, each of which is likely executing on a separate physical processor. In other words, scalability is achieved through sheer distribution.

One limitation, of course, is that not all problems can be easily parallelized in this manner. Unless the *problem* is naturally, easily parallelized, increasing the scale can happen at the significant expense of efficiency.

#### Place the data sources close to the data consumers.

If components that need to access some data are distributed across a network, the decision to have a single, remotely located data storage component will result in a lot of network traffic. In turn, this will affect the system's performance. It will also affect its ability to accommodate additional client components that may yet further increase the data traffic. One solution is to always keep the data sources close to data consumers, minimizing the resulting network traffic, and even co-locating them on the same host whenever possible.

Clearly, this guideline will be difficult to apply in many distributed systems. Moving the data closer to the processing components can be done virtually through techniques such as caching and pre-fetching, as discussed earlier. However, in such cases the system needs to ensure that multiple copies of the same data are synchronized, which may add to the system's processing and communications load beyond the savings incurred by making data accessing local.

Another possibility is to co-locate the processing components. However, the application's location constraints may limit the architect's options. Furthermore, even if a given component could be redeployed to another host (that is, closer to the data), its interactions with other parts of the system may suffer as a result.

#### Try to make distribution transparent.

Relocating either processing or data to improve a system's performance or scalability in the manner discussed above requires some degree of location transparency. We have discussed the potential negative impact of a component's location transparency on efficiency. At the same time, location transparency can aid a system's scalability.

In a distributed setting, scaling up a system will often result in changing the deployment view of the system's architecture. For example, new users may need to be allowed to access the system via new hardware hosts. Processing or data components may need to be added in specific places in the architecture, or they may need to be relocated across hosts, to enable

the new users. The outcome will be increased processing and data traffic in the system.

Redeployment may cause significant disturbances to a system. However, if connectors are capable of handling both local and remote interactions in a manner that is transparent to the involved components, then the system can be reconfigured in several ways, such as by redeploying consumer components closer to the needed data sources, replicating remote functionality locally for performance, or off-loading components to capacious remote hosts.

The impact of such adaptations always needs to be assessed carefully before they are effected.

#### **Use appropriate architectural styles.**

The architectural styles selected for a given system will have a significant influence on that system's scalability. As has been the case with other system properties, even if we do not take into account specific details of the system under development, certain architectural styles will be more appropriate for achieving scalability than others. Thus, for example, publish-subscribe and event-based architectures have been demonstrated to scale to very large numbers of components, users, devices, and data volumes. Other styles typically result in systems that scale well in one or more dimensions. For example, interpreter-based systems cannot easily accommodate growing numbers of users, but can usually handle addition of new functional operators. Likewise, pipe-and-filter may be unable to support increasingly large volumes of data, but can support increasing numbers of components, since arbitrarily long pipelines can be constructed.

## **12.4 Adaptability**

**Definition.** *Adaptability* is a software system's ability to satisfy new requirements and adjust to new operating conditions during its lifetime.

Adaptability can be manual or automated. A software system's architecture has an impact on either type of adaptability. Since Chapter 14 is dedicated in its entirety to architectural adaptation, we will only make some general observations here.

### **12.4.1 Software Components and Adaptability**

Architecturally-relevant adaptability occurs at the level of system components, their interfaces, and their composition. In other words, if adaptation is required entirely *within* an individual component or connector, that adaptation is not considered to be architectural. Such adaptations can still be effected with the aid of the system's architecture, for example, by replacing an entire component with its newer version. This observation informs several guidelines for designing for adaptability.

#### **Give each component a single, clearly defined purpose.**

This guideline has been discussed above – twice! – in the context of efficiency and complexity. Since architecture-level adaptation occurs at the level of entire components, it is imperative to separate different system concerns into multiple components. This allows the architects and engineers to minimize the amount of degradation the system experiences during adaptation.

#### **Minimize component interdependencies.**

Adapting a complex system is difficult. Each modification may impact multiple parts of the system. For example, Figure 12-5 indicates that modifying any major subsystem of Linux will, in principle, have an effect on every other subsystem. Defining the system's components to have simple interfaces, in a manner that precludes unnecessary interdependencies, can help to control the effects of adaptation.

#### **Avoid burdening components with interaction responsibilities.**

Again, this guideline was discussed previously in the context of other NFPs. In the context of adaptability, the objective is to separate the system's functionality and data from interaction.

#### **Separate processing from data.**

Adaptations to the system's processing components should be handled independently of adaptations to its data.

#### **Separate data from metadata.**

Changes to the data in a large, long-lived software system will occur regularly. If the data is separated from the metadata (that is, the data about the data), then in principle each can be adapted independently of the other. Furthermore, the processing components will be able to adapt more easily to the changes in both the data and the metadata.

### 12.4.2 Software Connectors and Adaptability

Connectors are the key enablers of architectural adaptability. Components should be insulated from their particular context to the greatest extent possible in order to appropriately separate system concerns and maximize their reuse potential. It is the task of connectors to provide the necessary facilities that enable a given component to operate appropriately in its environment. Several guidelines for adaptability stem from this observation.

#### Give each connector a clearly defined responsibility.

If a connector is in charge of enabling the interactions of a given type among a specific set of components, it will be easier for architects and engineers to manage the required adaptations to those components or their interactions. However, this requires one additional property of connectors, discussed next.

#### Make the connectors flexible.

At least, connectors must be able to support different numbers of components, and possibly component types. If a connector is unable to do so by itself, composing it with other connectors may produce the desired effect, as elaborated next.

#### Support connector composability.

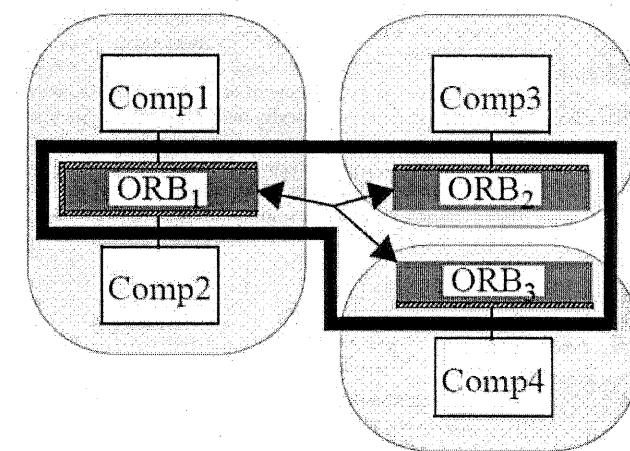
In order to enable interactions among heterogeneous components, which may be added to a system during runtime, connectors must be composable with other connectors. For example, Figure 12-6 shows a connector composed from three separate object request brokers (ORBs) – recall the discussion on CORBA from Chapter 4. In the architecture depicted in Figure 12-6 each component only exchanges information with the connector to which it is directly attached; in turn, the connector will (re)package that information and deliver it to its recipients using one or more middleware technologies – whatever is necessary to achieve communication. Each such middleware-enabled connector exposes the interface expected by its attached components. The connector may change the underlying mechanism for marshalling and delivering messages, but externally appears unchanged.

Such a composite connector has the added advantage that it can also preserve the topological and stylistic constraints of the application. For example, the application in Figure 12-6 was designed according to the C2 style (recall Chapter 4). This means that, for example, components *Comp1* and *Comp2* can interact with one another, while *Comp1* and *Comp3*

cannot. Using a single ORB to connect the components—even if it were possible—would potentially violate these stylistic constraints.

Another advantage of such composite connectors is that they are independent of other connectors in the system, and can optimize aspects of communication in a homogeneous setting (e.g., if the interaction between *Comp1* and *Comp2* is local). Maintaining a connector's interface and semantics, coupled with its composability, allows much more flexibility in application development and deployment. For instance, if it were later decided that *Comp3* and *Comp4* should indeed run in the same process, it would be possible to make this change by simply reconfiguring the composite connector. The component code would not have to be changed at all.

Figure 12-6. A software system that has been distributed across three hardware hosts, which are represented by the lightly shaded ovals. The system's four components interact through a single conceptual connector.



denote  
d by  
the  
polygo  
n  
spanni  
ng the  
.three  
hosts.  
This  
connec  
tor is  
actuall  
y  
compo  
sed  
from  
three  
interac  
ting  
object  
reques  
t  
broker  
s  
(ORBs  
). The  
three  
ORBs  
may  
be,  
e.g.,  
differe  
nt  
CORB  
A  
imple  
mentat  
ions,  
or they  
may  
repres  
ent  
arbitra  
ry  
middle  
ware  
platfor  
ms.  
Each  
ORB  
export  
s the  
interfa

ces  
expect  
ed by  
its  
attache  
d  
compo  
nents.  
To do  
so, the  
differe  
nt  
ORBs  
may  
need to  
include  
adapto  
rs,  
depict  
ed as  
highlig  
hted  
ORB  
edges,  
in  
order  
to  
enable  
the  
compo  
nents'  
interop  
erabilit  
y.

#### **Be aware of differences between direct and indirect dependencies.**

This guideline has been discussed above in the context of scalability. Much of the argument is applicable for adaptability. In principle, direct and explicit dependencies result in more efficient systems, while indirect and implicit dependencies allow the given system to adapt more easily.

#### **12.4.3 Architectural Configurations and Adaptability**

##### **Leverage explicit connectors.**

A software system in which the connectors are implicit (that is, in which components are endowed with interaction capabilities) will be difficult to

adapt since individual concerns may be distributed across multiple system elements.

#### Try to make distribution transparent.

As in the case of scalability, distribution transparency has its advantages when adaptability is concerned: making modifications to a system is much easier if components are oblivious to the system's deployment profile. For example, the system or one of its parts may be redeployed without requiring changes to the system's components. Of course, the efficiency impact of such adaptations must be carefully taken into account.

#### Use appropriate architectural styles.

As with other NFPs, architectural patterns and styles can directly impact adaptability. Simply put, certain styles are better suited to support adaptability than others. For example, styles that support event-based interaction, such as publish-subscribe and implicit invocation, naturally and effectively support adaptability. On the other hand, styles that require direct dependencies among the components, such as virtual machines or distributed objects, can hamper adaptability.

## 12.5 Dependability

Littlewood and Strigini define dependability informally as a collection of system properties that allows one to rely on a system functioning as required [166]. Dependability is a composite NFP which encompasses several other, related NFPs: reliability, availability, robustness, fault-tolerance, survivability, safety, and security. Security is discussed in detail in the next chapter. Here we focus on the design guidelines required to ensure the remaining facets of dependability in a system's software architecture.

We first provide several definitions, which illustrate the inter-related nature of these different facets of dependability. We then discuss the role of software architecture in ensuring a software system's dependability.

**Definition.** A software system's *reliability* is the probability that the system will perform its intended functionality under specified design limits, without failure, over a given time period.

**Definition.** A software system's *availability* is the probability that the system is operational at a particular time.

Unlike reliability, which is a statistical measure of the system's overall health over a continuous period of time, availability represents the system's health at discrete snapshots in time.

**Definition.** A software system is *robust* if it is able to respond adequately to unanticipated runtime conditions.

Robustness deals with those runtime circumstances that have not been captured in a system's requirements specification. It can be said that responding to conditions specified in the requirements is a matter of system correctness, while responding to all other conditions is a matter of robustness. The adequacy of the response will vary depending on different factors, such as application domain, user, and execution context.

**Definition.** A software system is *fault-tolerant* if it is able to respond gracefully to failures at runtime.

The failures affecting a system can be outside the system itself, whether caused by hardware malfunctions or system software defects, such as network or device driver failures. Alternatively, the system's own components may fail due to internal defects. What constitutes a graceful reaction to failure will depend on the system context. For example, one system may continue operating in a degraded mode; another one may introduce, possibly only temporarily, new copies of the failed components; yet another may offer the "blue screen of death" to the consternation of its users, requiring a reboot of the entire computer, after which the user might be able to continue with normal operation.

From a software architectural perspective, faults can be classified into the following:

1. faults in the system's environment (that is, outside the software architecture),
2. faults in components,
3. faults in connectors, and
4. component-connector mismatches.

An NFP closely related to fault-tolerance is survivability.

**Definition.** *Survivability* is a software system's ability to resist, recognize, recover from, and adapt to mission-compromising threats.

Survivability must address three basic kinds of threats:

1. *attacks*, examples of which are intrusions, probes, and denials-of-service,

2. *failures*, which can be due to system deficiencies, or defects in external elements on which the system depends, and
3. *accidents*, which are randomly occurring but potentially damaging events such as natural disasters.

Therefore, fault tolerance and survivability are related because the goal of both is to effectively combat threats, and system faults can be viewed as one kind of threat.

It should be noted that the distinction between the three categories of threats may not matter in the context of recovery from the threats. The key to survivability is to try to recover from these threats as gracefully as possible. In order to make a system survivable, the basic activities that can be performed are

1. resistance to threats,
2. recognition of threat and extent of damage,
3. recovery of full and essential services after a threat, and
4. adaptation and evolution to reduce the impact of future attacks.

The final facet of dependability that will be discussed in this chapter is software system safety. Several definitions of software safety are currently in use. These are usually variations on the definition provided by Leveson [164]. We provide a similar definition.

**Definition.** *Safety* denotes the ability of a software system to avoid failures that will result in loss of life, injury, significant damage to property, or destruction of property.

It should be noted that different degrees of property damage and destruction, and even human injury, may be considered acceptable in the context of different systems and/or system usage scenarios. The elaboration of such circumstances is outside the scope of this book, however.

The remainder of this section offers several guidelines for a software architect to follow in order to improve the resulting system's dependability.

### 12.5.1 Software Components and Dependability

More dependable software components will, on the average, result in more dependable software systems – though it should be noted that dependable components need not always result in dependable systems, and that highly dependable systems may comprise undependable individual components (recall the “Honey-Baked Ham” sidebar in Chapter 8). Practice has shown that it is seldom possible to develop components that are completely reliable, robust, and fault-tolerant. However, engineers can follow certain practices to help with achieving these properties. In particular the

guidelines below are targeted at the outwardly visible facets of a component.

#### Carefully control external component inter-dependencies.

Changes in the behavior of a given component, including anomalous behavior and failures, should have a minimal impact on the remaining components in the system. This can be achieved by properly insulating components from one another. One specific guideline is to restrict all inter-component dependencies to be explicit and only at the level of the components' public interfaces. Recall from the discussion earlier in this chapter that following this guideline may compromise a system's scalability and adaptability. Another guideline is to minimize, or completely disallow, side effects from component operations.

#### Provide reflection capabilities in components.

While a given component in a system may be unable to provide certain desired dependability guarantees, it should be possible to partially mitigate that by enabling querying of the internal state of the component. This will allow other parts of the system to assess the health of the component at times that are deemed important.

#### Provide suitable exception handling mechanisms.

When an individual component fails, the rest of the system may be able to adjust to that failure. In order for that adjustment to happen quickly and gracefully, the failing component should be able to expose the necessary information to the rest of the system. One way of doing so is by providing exception reporting mechanisms via the component's public interface. This will allow the other components and connectors in the system to adjust their operation accordingly.

#### Specify the components' key state invariants.

Architects can explicitly state conditions that must hold at different times during the component's execution. Such invariants will allow the component's users to establish best-case, normative, and worst-case guarantees when interacting with that component. Different actions taken in response to that information will then have the potential to improve the overall system's dependability.

## 12.5.2 Software Connectors and Dependability

### **Employ connectors that strictly control component dependencies.**

Unintended or implicit dependencies among a system's components will likely harm a system's dependability. Explicit, first-class connectors can be used to manage all dependencies among system components. If necessary, connectors can completely insulate components from one another. It should be noted that widely used connectors such as shared memory and procedure calls give developers too much leeway in creating component interdependencies. Many distributed systems employ connectors that, by necessity, strictly enforce component boundaries and control remote interactions. However, the reader should recall from Chapter 5 that even within a single address space it is possible to leverage connectors, such as event buses, that will enforce any component interaction requirements.

### **Provide appropriate component interaction guarantees.**

In certain scenarios, it is imperative that a component receive the data sent to it, even if that means sending the information multiple times. In other scenarios, the system's hardware resources may be overtaxed to the point where, regardless of other needs, the system cannot afford to have the same data transmitted or processed more than once. In yet other circumstances, the recipient components may process each event, even though these are replicas of the same event. In that case, the system's state may erroneously change and the results produced may be wrong. This could have disastrous consequences in a safety-critical system: consider receiving, multiple times, a command to change the pitch, roll, or yaw of an aircraft by a specified value.

In large, distributed systems—especially those composed with heterogeneous, possibly off-the-shelf components—the individual components may, for instance, make different assumptions about each other, the desired interaction profiles, or the state of the hardware resources. In such situations it is the responsibility of connectors to ensure that all interaction guarantees (e.g., at least once, at most once, or exactly once) are provided, and possibly adapted in response to changing circumstances during the system's execution.

### **Support dependability techniques via advanced connectors.**

A number of dependability concerns and needs in a system cannot be met simply by constructing solid components, properly composing them, and ensuring that they interact only in the prescribed ways. Large, complex, distributed, embedded, and mobile systems need to respond to many external stimuli, and can suffer failures induced by human users, hardware

malfunctions, or interference – whether accidental or malicious – from other software systems.

To deal with such situations, connectors may need to support advanced interaction facilities. Examples include providing replicas of failing or failed components on the fly, runtime replacement of components (also referred to as “hot swaps”), and support for multiple versions of the same functionality, for example to ensure the correctness of calculations. These facilities will often need to be provided such that the system's existing, still correctly functioning components are unaware of them. In other words, connectors should support *seamless* dependability.

## 12.5.3 Architectural Configurations and Dependability

### **Avoid single points of failure.**

In many large systems, a large portion of a system may depend on the services provided by one component or a small number of components. If those services are critical to the system's mission, the failure of the component, or components, providing them will significantly or completely incapacitate the system.

There are numerous examples of such systems. For instance, any data-intensive system with a centralized repository cannot afford to lose the repository. Likewise, a spacecraft with a centralized controller will be lost if the controller fails. Yet another example is a swarm of robots relying on a centralized planning engine; the robots may end up roaming aimlessly if the planner malfunctions.

There are several techniques that can be employed to deal with such concerns, including replicating the component in question, clearly separating into multiple components the different concerns it may embody, and employing connectors with advanced capabilities such as those discussed immediately above. At the same time, it should be acknowledged that in some situations it may be impossible to avoid creating a design that contains one or more single points of failure. Regardless of the circumstances (that is, whether the single point of failure can be avoided or not), software architects need to be aware of this issue throughout the design process.

### **Provide back-ups of critical functionality and data.**

This guideline should be obvious. It is also not universally applicable. For example, it is possible that a lack of system resources or hard real-time constraints effectively prevent back-ups. However, as with one's personal computer or PDA, back-ups are ultimately the best way of ensuring that

critical functionality and data are not lost. Different techniques may be used to implement this guideline, including employing advanced connectors such as those discussed above.

#### **Support non-intrusive system health monitoring.**

It may be too late to try to deal with system malfunctions once they have already occurred. Frequently, however, a system will exhibit anomalous behavior and give hints that something is wrong for some time before it, or a part of it, actually fails. Periodically monitoring the system for certain events that indicate its health status can help engineers to anticipate, and possibly eliminate, any unexpected behavior.

Non-intrusive monitoring can be achieved in a number of different ways. One possibility is to employ a component model that supports including explicit monitors at the level of application components. Another, even less intrusive possibility is to include monitoring facilities within the system's connectors. Component containers used in many middleware platforms present another possible target for placing system health monitors.

#### **Support dynamic adaptation.**

A dynamically adaptable system is able to respond to events at runtime; a static system may not. Dynamically adaptable systems are able to support the addition, removal, replacement, and reconnection of both components and connectors while the system is running. In decentralized settings they frequently also support dynamic discovery of available services. A thorough treatment of the role of software architecture in dynamic adaptation is provided in Chapter 14.

It should be noted that dynamic adaptation can harm a system's dependability, at least temporarily. The reader should recall the discussion of mobility in Chapter 10, and in particular of the diagram in Figure 12. In addition to rendering the system at least temporarily undependable *during* the dynamic adaptation, it is possible that the result of adaptation will be a system whose critical properties, including its dependability, are compromised. This is a reason why the stakeholders of many highly safety-critical systems are leery of dynamically modifying their systems. In other words, while dynamic adaptation can be a very useful tool at an architect's disposal, it should be applied with caution!

## **12.6 End Matter**

Engineering a software system to provide the required functionality is often quite challenging. This is why historically a majority of the software

design and implementation techniques have focused on supporting and improving a system's functional capabilities. Ultimately, however, good engineers will usually manage to produce almost any functionality, no matter how complex. What they will still struggle with are the non-functional aspects of their systems.

Recall the discussion of the "better-cheaper-faster – pick any two" software engineering maxim from Chapter 10. It suggests that, so long as the system stakeholders are willing to sacrifice one or more of the system's non-functional characteristics, such as schedule, cost, or performance, developers will be able to produce the desired functional capabilities.

Producing those capabilities *along with* the desired non-functional system characteristics is significantly more challenging. There is much less guidance available, in particular to software system architects, for how such characteristics are to be "designed into" the system in question. One reason is that many of these characteristics are loosely defined and qualitative in nature. The challenge becomes even more daunting when system stakeholders have to consider multiple, possibly clashing non-functional characteristics simultaneously.

This chapter has distilled a large body of experience and good software engineering practices into a set of guidelines (or "tactics", as they have been referred to elsewhere in literature, e.g., [246]) that software architects can follow in achieving specific non-functional properties. The guidelines should work most of the time, but they should be applied with caution. Whenever appropriate, each of the guidelines in this chapter has been coupled with specific admonitions that reflect the difficulties a software architect may encounter in certain development scenarios.

The reader should keep both the guidelines and the accompanying admonitions in mind when designing software systems. The reader should also realize that this chapter did not, and could not, provide a complete enumeration of all possible architectural design scenarios, or all possible trade-offs among the choices made in achieving the desired non-functional characteristics.

#### **The Business Case**

Achieving desired non-functional properties often makes the difference between a successful product and a failure. There are many examples from the software development industry. The reader just need recall the example of Microsoft Word 6.0, released in the mid-1990s. The Windows version of the product performed well and was successful. The Macintosh version, with roughly the same functionality, was large and slow, and resulted in a fair amount of bad publicity for Microsoft. This example is

telling also in that attempts at patching the product proved unsuccessful, so that Microsoft eventually had to revert to Word 5.0 for its Macintosh user base.

While Microsoft was able to weather this particular storm, a smaller company in its place may not have been able to recover as easily. “Inserting” a non-functional property into a system after the system has been designed, and possibly implemented, is rarely a successful strategy, and it is fraught with dangers. A much more appropriate approach is to plan for the desired properties from the project’s inception and to ensure that the necessary architectural design decisions are made. In many situations, even knowing what *not* to do, or at least which pitfalls to avoid, in the system’s design can be quite valuable. The guidelines provided in this chapter can serve as a useful tool in that regard.

## 12.7 Review Questions

1. Define the following NFPs:
  - a. efficiency
  - b. complexity
  - c. adaptability
  - d. scalability
2. What are the different dimensions of dependability?
3. How is each of the above NFPs manifested in software architectures?
4. How can each of the above NFPs be addressed at the architectural level?
5. Identify at least three guidelines for achieving each of the above NFPs. Elaborate on the manner in which each of those guidelines supports the NFP in question.
6. Can multiple NFPs be achieved simultaneously? If so, under what conditions? If not, why not?

## 12.8 Exercises

1. It is often difficult to simultaneously satisfy multiple non-functional properties (NFPs). Discuss the trade-offs between the following NFPs with respect to their impact on a system’s architecture. For each trade-off, provide the answer in three parts: discuss how your architectural choices can help to maximize each of the two individual properties (possibly at the expense of the other property); then discuss architectural choices that can help you maximize both properties in tandem. Make sure to provide

your answer at least in terms of the role and specific characteristics of components and connectors that impact the NFPs.

- a. performance vs. complexity
- b. safety vs. efficiency
- c. reliability vs. adaptability
2. Recall the example Lunar Lander architectures discussed in Chapter 4. Select any two of the architectures from Chapter 4. For each NFP discussed in this chapter, analyze what can (and cannot) be determined about the selected architectures. Can you recognize any of the NFP design guidelines in either of the two architectures? What is your assessment of the architectures’ respective support for the NFP under consideration?
3. Now consider an ADL model of Lunar Lander from Chapter 6. Does the model aid or hamper your ability to answer the questions from the preceding exercise? Be sure to justify your answer.
4. Discuss how one of the architectures selected in the two preceding exercises can be adapted to improve
  - a. efficiency
  - b. scalability
  - c. adaptability
5. The list of guidelines for achieving the different NFPs provided in this chapter is incomplete. Add at least one additional guideline for each existing NFP.
6. Devise a set of design guidelines for achieving additional properties, such as
  - a. heterogeneity
  - b. compositionality
  - c. security

If necessary, you should locate the definitions and any other necessary explanation of these properties. Note that security is discussed in Chapter 13.
7. Analyze the pair-wise trade-offs among one the properties you devised in the previous exercise and those introduced in this chapter.

## 12.9 Further Reading

Several software engineering textbooks provide useful overviews of non-functional properties (NFPs). Ghezzi, Jazayeri, and Mandrioli [96] are particularly thorough in their treatment of NFPs. They divide the NFPs into internal (relevant to architects and developers) and external (relevant to customers and users). Furthermore, they divide NFPs into those relevant to the developed product and those relevant to the development process. The NFPs studied in this chapter are the internal product NFPs.

Ghezzi et al. do not focus on the design guidelines for accomplishing the various NFPs. A recent book by Rozanski and Woods[246] attempts to do just that. The authors identify a set of NFPs relevant to software architects. These include performance, scalability, security, and availability. They also propose a number of guidelines, called tactics, targeted at achieving the NFPs. Several of their tactics are relatively general (e.g., “capture the availability requirements”), and are not targeted separately at different architectural facets such as components, connectors, and configurations.

A volume on the Future of Software Engineering (FoSE) [77], accompanying the Proceedings of the 22<sup>nd</sup> International Conference on Software Engineering (ICSE 2000), provided a set of useful overviews and research roadmaps for several NFPs, including reliability and dependability[166], performance [232], and safety [172]. These topics have been revisited in the FoSE volume [29] accompanying the 29<sup>th</sup> International Conference on Software Engineering (ICSE 2007) by Lyu (reliability) [173], Woodside et al. (performance)[305], and Heimdahl (safety) [115].

Many of the architectural guidelines advocated in this chapter targeted at accomplishing NFPs emerged over time from general software engineering principles. For example, modularity and separation of concerns was articulated by Parnas over thirty years ago [219]. More recently, DeLine has argued for a de-coupling of a component’s “essence” from its “packaging” [57]. Allen, Garlan, and Ockerbloom have shared a very useful experience on the effects of off-the-shelf component integration on a system’s NFPs, and the inherent architectural causes [87, 88].

## CHAPTER 13

# 13 Security and Trust

The preceding chapter introduced several non-functional properties (NFPs) and described how addressing those properties at the software architectural level helps yield a software system that effectively exhibits them. Security is one such critical property; its increasing need and importance warrants the in-depth look provided in this chapter. As with many other properties, it is most effectively addressed while designing the architecture of a system. Consider the example of building architectures discussed in Chapter 1. A building is designed with various structural properties and the owner’s requirements in mind. However, if the building has windows or doors that are easy to access from the outside, or its structure prevents the installation of security alarms, the building becomes vulnerable to potential thieves. If these considerations are addressed during the building’s design, an effective structure at a reasonable price is achievable.

If the building is not designed from the outset with security in mind, it may still be possible to add external reinforcements to improve security when such demands occur. For example, thin walls can be reinforced by adding extra layers; doors and windows that represent potential points of entry can be safeguarded using suitable lock and key mechanisms. In some cases, a building may not be secure by itself against thieves but it might be housed within a gated community which safeguards the entire community against external thieves.

The caveat of adding security afterwards, though, is that it is generally more expensive than what would be if the proper measures had been taken from the beginning. Imagine opening up the walls, installing extra wires and cameras, and then closing the walls. This is more expensive than envisioning the requirements from the start and designing the building around those requirements. The same is true for software. It is therefore imperative that security be considered and treated at the system architectural level. Using a software architecture-based approach for security allows developers to leverage experienced benefits and achieve guaranteed security properties. Software architecture also provides a sound basis for the reasoning and analysis of security properties.

Note that while external reinforcements can be used to provide a certain degree of security post-development, it still entails that the software be designed to allow addition of such reinforcements without compromising required functionalities. This makes reasoning about security at the architectural level even more crucial. Further, since software systems often go through an extended round of releases as new functionalities are added, a security-based architectural approach can provide guidance through the various software evolution cycles and help ensure that essential security properties continue to be achieved through each release.

The typically unsatisfactory realization of software security stems in part from the adoption of a common mechanism to build software systems as well as from the environment in which these systems are deployed and operated. Many systems are built from pre-existing components that may originate from different sources. This complicates analysis and composition even when a dominant composition mechanism is available. Additionally, more and more software is running in a networked environment. Such systems interact over the network with other systems that they do not always control or fully trust. Fast and always-on network connections provide opportunities for malicious attacks that were not previously possible. These situations raise new challenges for how secure software should be developed.

Security, as important as it is, is only a part of the overall system. It has to be balanced with other non-functional properties. For example, encryption is generally used in software systems to keep data secret, but using encryption can be computationally expensive, and the performance of the system might be adversely impacted by such operations. Even more importantly, security, along with other non-functional properties, must be balanced against a system's general functional requirements. For example, a browser that displays and executes all types of content would provide the richest experience for users, but such indiscreet execution is almost doomed to bring malicious software into a user's computer. When facing such choices, uninformed stakeholders, such as end users and product planning teams, might choose functionalities over other critical properties. A software architecture approach can ameliorate this condition by providing the necessary abstraction and tools that will help stakeholders to make sound decisions.

In this chapter, we will first introduce the different aspects of security, including confidentiality, integrity, and availability. Then, we will discuss several general design principles for security. These principles have been developed by theoreticians and practitioners over the years and have been applied to many software systems. We will illustrate how these principles can be applied to software architectures. Next, we will discuss a technique

for architectural access control. This technique complements traditional software architecture techniques with capabilities to specify and regulate inter-component communication. Finally, we will conclude this chapter by presenting a software architectural approach for constructing trust-enabled decentralized applications. These types of applications play an important role in the emerging collaborative Web world, where autonomous users communicate and collaborate frequently in a community environment and require trust management to protect themselves from other malicious users.

Outline of Chapter 13	<ul style="list-style-type: none"> <li>13 Security and Trust</li> <li>  13.1 Security</li> <li>  13.2 Design Principles</li> <li>  13.3 Architectural Access Control</li> <li>    13.3.1 Access Control Models</li> <li>    13.3.2 Connector-Centric Architectural Access Control</li> <li>  13.4 Trust Management</li> <li>    13.4.1 Trust</li> <li>    13.4.2 Trust Model</li> <li>    13.4.3 Reputation-based Systems</li> <li>    13.4.4 Architectural Approach to Decentralized Trust Management</li> <li>  13.5 End Matter: Trade-offs</li> <li>  13.6 Review Questions</li> <li>  13.7 Exercises</li> <li>  13.8 Further Reading</li> </ul>
-----------------------	---

## 13.1 Security

The National Institute of Standards and Technology defines computer security as “The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).” [107] According to this definition, there are three main aspects of security: confidentiality, integrity, and availability. We briefly introduce them here. For a comprehensive treatment, see the Related Work discussion at the end of the chapter for specific references.

### Confidentiality

Preserving the confidentiality of information means preventing unauthorized parties from accessing the information or perhaps even being aware of the existence of the information. Confidentiality is also referred to as secrecy.

A well-known effective measure to implement secrecy in software systems is through the use of encryption and decryption techniques. Cryptography itself has been used since the beginning of civilization, and the wide use of computer systems facilitates the wide adoption of computer cryptography.

A basic encryption mechanism can be described with the following equations:

$$\begin{aligned}\text{Cipher} &= \text{EncryptionFunction}(\text{Encryption\_Key}, \text{ClearText}) \\ \text{DecryptionFunction}(\text{DecryptionKey}, \text{Cipher}) &= \text{ClearText}\end{aligned}$$

When information needs to be encrypted to preserve confidentiality during communication or storage, the information, called clear text, is fed into an encryption algorithm, along with an encryption key, to produce a cipher. To retrieve the original information stored in the cipher, the cipher can be fed into a decryption algorithm, along with the decryption key, to produce the original clear text.

An encryption function has a corresponding decryption function. After using one encryption function, only the corresponding decryption function can be used to decrypt the cipher.

There are two forms of cryptography functions. With *shared key cryptography* the same key is used by both the encryption and decryption functions. This type of scheme has been used since the earliest days of cryptography. Management of the shared key presents problems, however. Since the key is shared between the sender and the receiver, the key must be delivered to both the sender and the receiver, which can be awkward if a sender wants to communicate with many receivers. Moreover since best security practices demand that keys not be reused (in order to defeat crypto analysis efforts by opponents), these key deliveries must be performed every time a key is changed.

To solve the key management problem with the shared key scheme, *public key cryptography* was invented in 1970s. These systems use a key pair, which consists of two related keys that are generated at the same time. One key, the private key, is retained and kept secret by an individual party. The corresponding key, the public key, is published by the individual and shared with everyone. To send information secretly, the initiator encrypts the clear text with the public key of the *recipient*, and send the cipher text. The recipient's private key is used by the individual to decrypt the message. If the keys are appropriately generated it is computationally infeasible for a third party to determine the individual's private key from the known public key, hence confidential communication

is assured.

Besides secrecy, public key cryptography can also be used to provide non-repudiation. The private key can be used to generate a digital signature. Such a signature is similar to a regular handwritten signature in that only the person who possesses the private key can generate the signature. Thus, receiving information having such a digital signature is a sure sign that the sender has sent the information, since no one can generate the signature without the private key. Recipients can use the sender's public key to verify signatures, thus establishing that the information was indeed sent by the sender (non-repudiation) and that it is authentic and was not tampered or modified along the way.

While a public key mechanism is flexible and mathematically sound, it suffers from a performance problem. It is generally orders of magnitude slower than a shared key algorithm. Thus, a choice exists between private key and public key: the former is fast, but is inflexible, and requires complex key management mechanism; the latter provides scalability and ease of management, but is much slower. An architectural solution that combines both of them is to use a public key mechanism to negotiate a shared key in the beginning of the communication session, and then apply the negotiated key with a shared key encryption algorithm in the ensuing communications.

An important lesson while designing a cryptography-based system is to avoid designing your own encryption algorithm. Such a design requires extensive mathematical skills, which is outside the scope of most projects. If you think you can design a secret encryption algorithm that no one knows, then the principle "do not depend on secrecy for security" is applicable here. It is almost inevitable that a determined hacker can expose the operational details of the newly proposed algorithm, and the "security" based on secrecy is lost. Instead, to design secure software based on cryptography to achieve secrecy and non-repudiation, a designer should evaluate the performance, architecture, and security requirements, choose a suitable, public algorithm, and use frequently changing keys as the primary secrecy mechanism.

This concept is as applicable to the domain of building architectures as it is to computer systems. For example, in a large office complex having two buildings, if the office management does not want others to know when certain items are moved between the two buildings, the management could build a covered passage between them such that others outside the building are unable to see what is moved within the passage. Even better, the passage could be built underground so people would not even be aware of the existence of the passage.

Applying this concept to software architectures, software components should take proper measures while exchanging information to protect confidential information from being intercepted by rogue parties. Likewise, software components should store sensitive data in a secure way so unauthorized users cannot discover the content or even the existence of such data.

### **Integrity**

Maintaining the integrity of information means that only authorized parties can manipulate the information and do so only in authorized ways. For example, in a building protected by a door that can be opened by entering an access code on a numeric panel, only the owner should be able to change the code. Moreover, when the code is changed, it should only be changeable to another numeric code – not to an alphanumeric one.

Analogous constructs exist at the programming language level, such as access modifiers of member fields and functions. For example, in Java, member fields and functions are given access levels as `private`, `package`, `protected`, and `public`, such that only certain parts of the class hierarchy can access those members. A private field of a class can only be accessed by the methods of the same class, whereas a package method can be called by all classes of the same package. Likewise, in C++, `const` pointers can be defined that enforce the condition that data accessed through those pointers cannot be changed.

At the software component and architectural level, a similar protective mechanism can be applied to the interfaces of components and their configurations through connectors. For example, if a particular interface of a component changes the most critical aspect of that component, the invocation of that interface should be limited to only those components that are authorized to do so. Therefore, such an interface should probably be separated from the others and receive more scrutiny during design.

To establish the identity of a user – and hence to determine whether the user is authorized or not – an authentication process is used to verify that the user is really who he claims to be. The most common form of authentication is the username/password pair: if a user can correctly supply the password associated with his username, then the user is successfully authenticated as that specific user. This is a form of authentication that relies on what a user knows; other forms of authentication include checking who the user is (for example, by scanning the iris of the user and comparing it to a set of authorized irises) and what the user has (for example, a user must possess a security token that can generate the correct number at the correct time.)

Depending on the security requirements, different levels of authentication may be used for software components and connectors. For example, in the Microsoft DCOM middleware technology, authentication may be bypassed completely. However, if needed, authentication can be performed at the beginning of a communication session, for each method, or even for each communication packet. The most secure authentication level is, of course, the packet authentication level, but it is also the most computationally expensive. The authentication requirement is handled by the DCOM middleware connector based on the authentication requirements of the communicating client and server. The middleware connector assures that both of them can operate on the chosen authentication level.

To deter potential intruders, a software system can maintain an audit trail that records important historical information. This can be better understood through the following analogy: the security guard of a gated community can record every visitor's name, license plate, and visiting time, so a security incident can be correlated to possible suspects. Likewise, security cameras can be deployed to record the activities of residents. Of course, such measures have to be balanced against privacy requirements.

Similarly, in the case of architectural components, audit trails can be maintained internally, i.e., the component may log requests and responses from an authenticated user and then produce an audit trail of those requests and responses at a later time. Connectors may also be used to log component invocations which pass through the connector. Further, since the architecture provides a system-wide view of the configuration of components and connectors, an audit trail can be captured recording patterns of access through the system.

### **Availability**

Resources are *available* if they are accessible by authorized parties on all appropriate occasions. In contrast, if a system cannot deliver its services to its authorized users because of the activities of malicious users, then its services are unavailable; it is said to be under a denial of service (DoS) attack.

Applications that are distributed across a network, such as the Internet, may be susceptible to a Distributed Denial of Service (DDoS) attack. Such attacks try to bring down the many distributed elements of an application. For example, the domain name system (DNS), which is in charge of resolving human-readable names (URLs) to computer-readable network addresses (IP addresses) and is distributed across different levels of operation, has occasionally been the target of such attacks. When such attacks succeed, access to web resources, for example, are frequently denied.

## 13.2 Design Principles

Security aspects of software systems should be considered from a project's start. During system conception the security requirements should be identified and corresponding security measures designed. Patching security after a system is built can be prohibitively expensive, if not infeasible. Security requirements also evolve with other requirements. Thus, an architect should anticipate possible changes and design flexibility into the security architecture. The architecture of the system is the place for software developers to identify the security requirements, design security solutions, and design to accommodate future changes.

In this section, we highlight several design principles that help guide the design of secure software. These principles emerged from the research community and have since been applied in many commercial software systems. Such principles are by no means sufficient by themselves for the design of secure software, but do play an important role in guiding designers and architects through possible alternatives and choosing an appropriate solution. These design principles are listed below and then described in detail.

- Least Privilege: give each component only the privileges it requires
- Fail-safe Defaults: deny access if explicit permission is absent
- Economy of Mechanism: adopt simple security mechanisms
- Complete Mediation: ensure every access is permitted
- Open Design: do not rely on secrecy for security
- Separation of Privilege: introduce multiple parties to avoid exploitation of privileges
- Least Common Mechanism: limit critical resource sharing to only a few mechanisms
- Psychological Acceptability: make security mechanisms usable
- Defense in Depth: have multiple layers of countermeasures

Principles adapted from Bishop [20], Saltzer & Schroeder [249], and Gasser [92].

### Principle of Least Privilege

The principle of least privilege states that a subject should be given only those privileges that it needs in order to complete its task. The rationale is that even if a subject is compromised, the attacker has access only to a limited set of privileges which limits the damage to certain specific parts of the system.

Currently, many less-informed Windows users browse the Internet using an account with many administrative privileges. This is not only unnecessary for the simple task of browsing the web but is potentially dangerous since it actually opens many paths for malicious software to take control of the user's computer. This practice owes its origin to early versions of Windows that were generally shipped with only one account, the administrator account. Based on the principle of least privilege, a minimally privileged account should be used for daily simple activities such as browsing and email. Embodying this principle, Internet Explorer 7, shipped in late 2006, can lower its privileges during execution to below those of the launching user's.

Software architecture makes it easier to determine the least privileges components should have. Explicit models of the architecture enable analysis of communication and control paths to determine the necessary attributes. A component should not be given more privileges than what is necessary for it to interact with other components.

### Principle of Fail-safe Defaults

The principle of fail-safe defaults states that unless a subject is granted explicit access to an object, it should be denied access to that object. This scheme might deny some safe requests that otherwise would have been granted, but it assures that each granted access is a safe access.

A simple illustration of this principle is the case of Internet browsers requesting a resource ("GETting a URL") on behalf of user's request. Fetching and displaying a web resource is a form of granting permissions based on the user-selected URL. Since a URL can be expressed and encoded in different forms (such as using absolute paths vs. relative paths), it is not always straightforward to list *all* invalid URLs and reject those. Thus, this rule suggests that accesses to all URLs should be denied unless their form can be verified as belonging to a known, valid kind.

Based on this principle, a connector connecting two components should only allow the specific communications that satisfy some approval criterion, rejecting all others.

### Principle of Economy of Mechanism

The principle of economy of mechanism states that security mechanisms should be as simple as possible – also referred as the KISS (Keep it Simple and Small) principle. While this rule generally is useful with any type of design, it is especially important for security systems. Complexity is the enemy of security since complex interactions make verifying the security of software systems more difficult and hence could possibly lead to a security breach.

One way to apply this principle is to isolate, consolidate, and minimize security controls. Redundant security mechanisms should be simplified. For example, in Internet Explorer prior to Version 7, there are multiple places where URLs are analyzed and results of these analyses are used to make decisions. Such redundancy and inconsistency led to security vulnerabilities. This issue was corrected in Internet Explorer Version 7 by centralizing the handling of URLs.

An architecture description provides a suitable abstraction to apply this principle more generally. It allows architects to analyze the locations of security controls, identify potential redundancy, and evaluate alternatives to choose a suitable place for the control.

#### **Principle of Complete Mediation**

The principle of complete mediation requires that all accesses to entities be checked to ensure that they are allowed, irrespective of who is accessing what. The check should also ensure that the attempted access does not violate any security properties.

Applying this principle to a software system requires all communication to be checked thoroughly. Such an inspection is greatly facilitated through the systematic view of the system provided by an accurate architectural model. A security architect can evaluate each possible interaction among the components in all types of configurations to make sure that none of the interactions and configurations violate the intended security rules.

The principle of economy of mechanism helps achieve complete mediation. Where there are only a limited number of security control mechanisms it is easier to apply security control, verifying that each access actually goes through these mechanisms.

#### **Principle of Open Design**

The principle of open design states that the security of a mechanism should not depend upon the secrecy of its design or implementation. While secrecy is a desired security property, secrecy itself should not be used as a mechanism. A secure design should not rely on the fact that an intruder does not know the internal operations of the software system. While keeping the internals secret might make it more difficult for an attacker to break into the system, simply relying on the such secrecy is unreliable. It is inevitable that such information will be discovered by malicious users in a world where many different types of information and computational resources are available to attackers. Trivially, employees could leak the secret, either intentionally or unintentionally. Among other options, the attacker can also try clever reverse engineering or simply brute force attacks.

Revealing the internals of a system can actually increase its security. In early stages of design other security reviewers can inspect and evaluate the design and provide insights. Further, during its operation and evolution phases, the system can be studied and refined accordingly to make it more secure. For instance, a system's security should not rely upon a software connector implementing a proprietary ("secret") communication mechanism. The likelihood of that idiosyncratic communication protocol having flaws is very high. Rather, using a protocol which has passed extensive external scrutiny is far more likely to provide the security desired.

#### **Principle of Separation of Privilege**

The principle of separation of privilege states that a system should not grant permission based on a single condition. It suggests that sensitive operations should require the cooperation of more than one key party. For example, a purchase order request generally should not be approved solely by the requestor, otherwise an unethical employee can keep requesting and approving inappropriate purchase orders without being detected for a long time.

Software architecture descriptions facilitate the checking of this principle. If a software architect discovers any component that possesses multiple privileges that should in fact be separated, the architect should redesign the architecture so that the privileges are partitioned between multiple components.

#### **Principle of Least Common Mechanism**

The principle of least common mechanism states that mechanisms used to access separate resources should not be shared. The objective of the principle is to avoid the situation where errors or compromises of the mechanism while accessing one resource allows compromise of all resources accessible by the mechanism. For instance, use of separate machines, separate networks, or virtual machines can help fulfill this principle and avoid cross-contamination.

In the context of software architectures, this means use of certain software architectural styles requires careful scrutiny. For example, in the case of the blackboard style, where all data is maintained on the shared blackboard and access to it is mediated by the blackboard component, the architect must ensure that the existence of the shared store and common mechanism does not introduce unintended security problems.

#### **Principle of Psychological Acceptability**

The principle of psychological acceptability states that security mechanisms should not make the resource more difficult to access for legitimate users than if the security mechanisms were not present. The

human interface of security mechanisms should be designed to match the mental model of the users and should be easily usable. Otherwise, the users will either attempt to bypass the security measure because it is too difficult to use or use it incorrectly because the user interface is error-prone.

This principle did not receive considerable attention in the past in the context of secure software design. However, now that software has become a mainstream phenomenon and most computer users are not technically savvy, it is becoming critical to design secure software keeping in mind the psychological acceptability of users.

By analogy, a building may have several security capabilities to safeguard it, such as specially designed door and security alarms, but if the building owner does not take advantage of those capabilities because it is too cumbersome or error-prone to turn on the security alarms, then essentially the building becomes as vulnerable to potential threats as those without such safeguards. With regard to software systems, an application may support security techniques such as digital authentication and cryptography, but if the end users do not utilize those techniques because they don't understand the mechanisms or cannot use the mechanisms correctly, the resulting system may become vulnerable to security attacks such as impersonation and repudiation.

The principle of psychological acceptability has been emphasized by Bruce Schneier, a security expert and the author of *Applied Cryptography* [251]. In his subsequent book *Secrets and Lies* [252] he writes,

Cryptography is a branch of mathematics. And like all mathematics, it involves numbers, equations, and logic. Security, palpable security that you or I might find useful in our lives, involves people: things people know, relationships between people, people and how they relate to machines. Digital security involves computers: complex, unstable, buggy computers.

Mathematics is perfect; reality is subjective. Mathematics is defined; computers are ornery. Mathematics is logical; people are erratic, capricious, and barely comprehensible.

The error of *Applied Cryptography* is that I didn't talk at all about the context. I talked about cryptography as if it were The Answer™. I was pretty naive.

The result wasn't pretty. Readers believed that cryptography was a kind of magic security dust that they could sprinkle over their

Bruce Schneier, on security systems, rather than security technologies

software and make it secure. That they could invoke magic spells like "128-bit key" and "public-key infrastructure." A colleague once told me that the world was full of bad security systems designed by people who read *Applied Cryptography*.

Since writing the book, I have made a living as a cryptography consultant: designing and analyzing security systems. To my initial surprise, I found that the weak points had nothing to do with the mathematics. They were in the hardware, the software, the networks, and the people. Beautiful pieces of mathematics were made irrelevant through bad programming, a lousy operating system, or someone's bad password choice. I learned to look beyond the cryptography, at the entire system, to find weaknesses. I started repeating a couple of sentiments you'll find throughout this book: "Security is a chain; it's only as secure as the weakest link." "Security is a process, not a product."

Any real-world system is a complicated series of interconnections. Security must permeate the system: its components and connections.

### Principle of Defense in Depth

The principle of defense in depth states that a system should have multiple defensive countermeasures in order to discourage potential attackers. Since an attacker will have to break through each of these countermeasures, it increases the likelihood of being able to identify and prevent an attack from occurring.

This principle requires each component in a path that leads to a critical component to implement proper security measures in its own context. This ensures that the security of the whole system will not be violated just because of one component's failure to implement proper security control.

A good example is the way Microsoft Internet Information Service (IIS) Version 6 (a web server) handles WebDAV requests. By re-architecting IIS, utilizing the underlying support provided by the operating system, and applying appropriate security measures at multiple points along the access path, IIS has become a far more secure system than its previous versions. The different mechanisms applied by different components along the WebDAV access path are shown in Figure 13-1.

POTENTIAL PROBLEM	PROTECTION MECHANISM	DESIGN PRINCIPLES
The underlying d11 (ntd11.dll) was not vulnerable because... Even if it were vulnerable...	Code was made more conservative during the Security Push. Internet Information Services (IIS) 6.0 is not running by default on Windows Server 2003. IIS 6.0 does not have WebDAV enabled by default. The maximum URL length in IIS 6.0 is 16 kbytes by default (> 64 kbytes needed for the exploit).	Check precondition Secure by default
Even if it were running... Even if Web-based Distributed Authoring and Versioning (WebDAV) had been enabled...	Secure by default Tighten precondition, secure by default	
Even if the buffer were large enough...	The process halts rather than executes malicious code due to buffer-overrun detection code inserted by the compiler.	Tighten postcondition, check precondition
Even if there were an exploitable buffer overrun...	It would have occurred in w3wp.exe, which is running as a network service (rather than as administrator).	Least privilege <small>(Data courtesy of David Aucsmith.)</small>

Figure 13-1.  
Security for  
Microsoft IIS

Table from [304]

This principle does not contradict the principle of economy of mechanism because it does not duplicate identical security checks, or worse, implement similar but inconsistent checks. Instead, each component provides its unique security safeguards that are most appropriate in its local context and thus helps to collectively form a more secure system.

### 13.3 Architectural Access Control

Having discussed the design principles for building secure software, we will now present one technique, namely, architectural access control, to demonstrate how software architects can follow the above-described principles in designing secure software systems. We will define the basic access control models in security, illustrate how these models can be applied at the software architectural level, introduce software tools that facilitate the utilization of these models, and through some examples show how these concepts and techniques can be practiced.

#### 13.3.1 Access Control Models

The most basic type of security mechanism used to enforce secure access is a *reference monitor*. The reference monitor controls access to protected resources and decides whether access should be granted or denied. The reference monitor is a *trusted computing base* (TCB) that is trusted to intercept every possible access from external subjects to the secured resources and to assure that the access does not violate any policy. Widely accepted practices require a reference monitor to be tamper-proof, non-by-passable, and small. A reference monitor should be tamper-proof so that it cannot be altered. It should be non-by-passable so that each access is mediated by the reference monitor. It should also be small so that it can be thoroughly verified.

Two dominant types of access control models are discretionary access control (DAC) models and mandatory access control (MAC) models. In a discretionary model, access is based on the identity of the requestor, the accessed resource, and whether the requestor has permission to access the resource. This permission can be granted or revoked at the resource owner's discretion. On the contrary, in a mandatory model, the access decision is made according to a policy specified by a central authority.

#### Classic Discretionary Access Control

The Access Matrix Model is the most commonly used discretionary access control model. It was first proposed by Lampson [160] and later formalized by Harrison, Ruzzo, and Ullmann [113]. In this model, a system contains a set of subjects (also called principals) that have privileges (also called permissions) and a set of objects on which these privileges can be exercised. An access matrix specifies the privilege a subject has on a particular object. The rows of the matrix correspond to the subjects, the columns correspond to the objects, and each cell lists the allowed privileges that the subject has on the object. The access matrix can be implemented directly resulting in an authorization table. More commonly, it is implemented as an access control list (ACL), where the matrix is stored by column, and each object has one column that specifies the privileges each subject has over the object. A less common implementation is a capability system, where the access matrix is stored by rows, and each subject has a row that specifies the privileges (capabilities) that the subject has over all objects.

#### Role-based Access Control

A Role-based Access Control Model (RBAC) is a more recent extension of the classic access control model. In this model, an extra level of indirection, called a role, is introduced. Roles become the entities that are authorized with permissions. Instead of authorizing a user's access to an object directly, the authorization is expressed as a role's permissions to an object and the user can be assigned to the corresponding role. RBAC allows roles to form a hierarchy. In such a hierarchical RBAC model, a senior role can inherit from a junior role. Every user that takes the senior role can also take the junior role, thus obtaining all the permissions associated with the junior role. The RBAC model, thus, eases management of access control in large-scale organizations. Instead of granting and revoking permissions individually to many users, all relevant users can be assigned a single role, and the permissions can be granted and revoked to this role. Role-based Access Control directly supports the principle of separation of duty. It also allows a clear specification of the roles that cannot be performed simultaneously by a user.

### Mandatory Access Control

Mandatory Access Control models are less common and more stringent than discretionary models. They can prevent both direct and indirect inappropriate access to a resource. The most common types of mandatory models work in a multi-level security (MLS) environment, which is typical in a military setting. In this environment, each subject (denoting a user) and each object are assigned a security label. These labels have a dominance relationship between them. For example, the “top-secret” label dominates the “classified information” label. A subject can only access that information whose label is dominated by the label of the subject. Thus, a subject with only “classified information” clearance cannot access “top secret” information while a subject with “top secret” clearance is able to access content that is labeled “classified information”.

#### 13.3.2 Connector-Centric Architectural Access Control

In this section, we present a connector-centric approach that describes how these access control models can be applied and enforced at the architectural level. Specifically, we describe how an architectural description can be extended to model security and how the resultant description can be checked to examine whether the architecture successfully addresses the security needs of the system.

##### Basic Concepts

The following core concepts are necessary to model access control at the architecture level: *subject*, *principal*, *resource*, *privilege*, *safeguard*, and *policy*.

##### *Subject*

A *subject* is the user on whose behalf a piece of software executes. The concept of subject is key in security, but is typically missing from software architectural models. Many software architectures assume that a) all of its components and connectors execute under the same subject, b) this subject can be determined at design-time, c) the subject generally will not change during runtime, either inadvertently or intentionally, and d) even if there is a change, it will have no impact on the software architecture. As a result, there is typically no modeling facility to capture the allowed subjects of architectural components and connectors.

Consequently, the allowed subjects cannot be checked against actual subjects at execution time to assure security conformance. In order to address these needs for architectural access control, basic component and connector constructs must be extended with the subject for which they perform, thus enabling architectural design and analysis based on different security subjects.

##### *Principal*

A subject can take upon multiple *principals*. Essentially, principals encapsulate the credentials that a subject possesses to acquire permissions. There are different types of credentials. In the classic access control model, the principal is synonymous with the subject and directly denotes the identity of the subject. But there exist other types of principals that provide indirection and abstraction necessary for more advanced access control models. In the Role-based Access Control model, each principal can denote one role that the user adopts. The results for accessing resources will vary depending on the different principals a subject possesses.

##### *Resource*

A *resource* is an entity for which access should be protected. Example resources and access controls on them are files which should be read-only, password databases that should only be modified by administrators, and ports that should only be opened by the root user. Traditionally, resources are *passive* and accessed by active software components operating for different subjects. However, in the case of software architecture, resources can also be *active*. Specifically, software components and connectors may also be considered resources, access to which should be protected. Such an active view is lacking in traditional architectural modeling. Explicitly enabling this view can give architects more analysis and design power to improve security assurance.

##### *Permission, Privilege and Safeguard*

*Permissions* describe possible operations on an object. A privilege describes what permissions a component possesses depending upon the executing subject. Privilege is another important security concept that is missing from traditional architecture description languages. Most current modeling approaches take a maximum privilege route wherein a component’s interfaces list all the privileges that that component could possibly need. This could become a source for privilege escalation vulnerabilities which are caused when a less privileged component is given more privileges than what it should be properly granted. A more disciplined modeling of privileges is therefore needed to reduce such vulnerabilities.

There are two types of privileges corresponding to the two types of resources. The first type handles passive resources and enumerates, for instance, which subject has read/write access to which files. The second type deals with active resources. These privileges include architecturally important privileges such as instantiation and destruction of architectural elements, connection of components with connectors, execution through message routing or procedure invocation, and reading and writing

architecturally critical information. These privileges are pivotal in assuring secure execution of software systems.

A notion corresponding to privilege is *safeguard*, which describes permissions that are required to access the interfaces of the protected components and connectors. A safeguard attached to a component or a connector specifies what privileges other components and connectors should possess before they can access the protected component or connector.

#### *Policy*

A *policy* ties together all the concepts defined so far. It specifies what privileges a subject, with a given set of principals, should have to access resources that are protected by safeguards. It is the foundation needed by the architectural elements to make access control decisions. Components and connectors consult the policy to decide whether an architectural access should be granted or denied.

#### **The Central Role of Architectural Connectors**

Architectural access control is centered on connectors. This is because connectors propagate privileges that are necessary for access control decisions. They regulate communication between components and can also support secure message routing.

#### *Components: Supply Security Contract*

A security *contract* specifies permissions an architectural element possesses to access other elements and the permissions other elements should possess to access the element. A contract is expressed through the privileges and safeguards of an architectural element.

In the ensuing discussion, for purposes of specificity, we will utilize and refer to modeling architectures using the xADL language [51], as presented in Chapter 6. For component types, the above modeling constructs are modeled as extensions to the base xADL types. The extended security modeling constructs describe the subject the component type acts for, the principals this component type can take, and the privileges the component type possesses.

The base xADL component type supplies interface signatures that describe the basic functionality of components of this type. These signatures become the active resources that should be protected. Thus, each interface signature is augmented with safeguards that specify the necessary privileges an accessing component should possess before the interfaces can be accessed.

#### *Connectors: Regulate and Enforce Contract*

Connectors play a key role in regulating and enforcing the security contract specified by components. They can determine the subjects the connected components are executing for. For example, in a normal SSL (secure socket layer) connector, the server authenticates itself to the client, thus the client knows the executing subject of the server. A stronger SSL connector can also require client authentication, thus both the server component and the client component know the executing subjects of each other.

Connectors also regulate whether components have sufficient privileges to communicate through the connectors. For example, a connector can use the information about the privileges of connected components to decide whether a component executing under a certain subject can deliver a request to the serving component. This regulation is subject to the policy specification of the connector. The recent version of DCOM, for example, introduces such regulation on local and remote connections.

Connectors can also potentially serve to provide secure interaction between insecure components. Since many components in component-based software engineering can only be used "as is" and many of them do not have corresponding security descriptions, a connector is a suitable place to assure appropriate security. A connector decides what communications are secure and should be allowed or what communications are dangerous and should be rejected or what communications are potentially insecure and require close monitoring.

#### **A Secure Architecture Description Language: Secure xADL**

Secure xADL is a secure software architecture description language that describes security properties of a software architecture. Secure xADL combines the xADL language with the architectural access control concepts defined in the preceding paragraphs. Figure 13-2 depicts the core syntax of Secure xADL. The central construct is *Security.PropertyType* which is a collection of the subject, the principals, the privileges, and the policies of an architectural element. The *Security.PropertyType* can be attached to component and connector types in xADL. Figure 13-2 illustrates that it is attached to a connector type to make a secure connector type. The *Security.PropertyType* can also be attached to components and connectors, making them secure components and connectors. Finally, the *Security.PropertyType* can also be attached to the specifications of sub-architectures and the description of the global software architecture.

Figure  
13-2.

```
<complexType name="Security.PropertyType">
<sequence>
```

**Secure  
xADL  
schem  
a**

```

<element name="subject"
         type="Subject"/>
<element name="principals"
         type="Principals"/>
<element name="privileges"
         type="Privileges"/>
<element name="policies"
         type="Policies"/>
</sequence>
</complexType>
<complexType name="SecureConnectorType">
<complexContent>
<extension base="ConnectorType">
<sequence>
<element name="security"
         type="SecurityPropertyType"/>
</sequence>
</extension>
</complexContent>
</complexType>
<complexType name="SecureSignature">
<complexContent>
<extension base="Signature">
<sequence>
<element name="safeguards"
         type="Safeguards"/>
</sequence>
</extension>
</complexContent>
</complexType>
<!-- similar constructs for component, structure, and
instance -->
```

An access control policy describes what access control requests should be permitted or denied. The policies for Secure xADL policies are embedded in the xADL syntax and written with the eXtensible Access Control Markup Language (XACML) [208]. XACML is an open standard from OASIS to describe access control policies for different types of applications. It is utilized in an environment where a policy enforcement point (PEP) asks a policy decision point (PDP) whether a request, expressed in XACML, should be permitted. The PDP consults its policy, also expressed in XACML and makes a decision. The decision can be one of the following: permit, deny, not applicable (when the PDP cannot find a policy that clearly gives a permit or a deny answer), and indeterminate (when the PDP encounters other errors).

The core XACML is based on the classic discretionary access control model where a request for performing an action on an object by a subject is permitted or denied. In XACML, an object is termed a resource. Syntactically, a PDP has a *PolicySet*, which consists of a set of

**Policy**. Each Policy in turn consists of a set of *Rule*. Each Rule decides whether a request from a subject for performing an action on a resource should be permitted or denied. When a PDP receives a request that contains attributes of the requesting subject, action, and resource, it tries to find a *matching Rule*, whose attributes match those of the request, from the *Policy* and *PolicySet*, and uses the matching rule to make a decision about permitting or denying access to the resource.

#### An Algorithm to Check Architectural Access Control

In xADL, each component and connector has a set of interfaces that represent externally accessible functionalities. An interface can be either an incoming interface, denoting functionality the element provides, or an outgoing interface, denoting functionality that the element requires. Each incoming interface can be protected by a set of safeguards that specify the permissions components or connectors must possess before they can access that interface. Each outgoing interface can also possess a set of privileges that is generally the same as those of the owning element, i.e. the privileges of the element having that outgoing interface.

The interfaces are connected to form a complete architecture topology. A pair of connected interfaces has one outgoing interface and one incoming interface. Such a connection defines that the element with the outgoing interface accesses the element at the incoming interface. Each such connection defines an *architectural access*. For example, in the C2 architecture style, a component sends a notification from its bottom interface to a top interface of a connector if the component has sufficient privileges. Architectural access is not limited to direct connections between interfaces. Two components could be connected through a connector. Thus, a meaningful architectural access might involve two components that only indirectly communicate through a connector.

At the architecture level, the concerning decision is whether an architectural access in a software architecture description should be granted or denied. More formally, this question should be answered: *given a software architecture description written in Secure xADL, for a pair of components (A,B), should A be allowed to access B?* Finding the answer to this question can help an architect design secure software from two different perspectives. First, the answer helps the architect decide whether the given architecture allows intended access control. If there is some access that is intended by the architect yet is not allowed by the description, the description should be changed to accommodate the access. Second, the answer can also help the architect decide whether there are architectural vulnerabilities that introduce undesired access. If some undesired access is allowed, then the architect must modify the architecture and architectural description to eliminate such vulnerabilities.

From an architectural modeling viewpoint, the security-related decisions made by components and connectors might be based on factors, or *Contexts*, other than the decision-maker and the protected resource. The four most common types of contexts that can affect access control decisions are: the neighboring components and connectors, the type of components and connectors, the sub-architecture containing components and connectors, and the global architecture.

An algorithm can be used to decide whether the outgoing interface of an accessing component carries sufficient privileges to satisfy the safeguards of the incoming interface of an accessed component. The accessing component can acquire privileges from multiple sources. The component may itself possess some privileges. It can also get privileges from its type, the containing sub-architecture, and the complete architectural model. Further, privileges can also propagate to the accessing component through connected components and connectors, subject to the privilege propagation capability of the connectors. The accessed components can acquire safeguards from similar sources. One notable difference in acquiring safeguards is that this process does not involve the connected element context, and thus does not go through a propagation process.

```

Input: an outgoing interface, Accessing,
and an incoming interface, Accessed

Output: grant if the Accessing can access
the Accessed, deny if the Accessing
cannot access the Accessed

Begin
  if (there is no path between Accessing
  and Accessed)
    return deny;
  if (Accessing and Accessed are connected
  directly)
    DirectAccessing = Accessing;
  else
    DirectAccessing = the element
      nearest to Accessed in the path;
  Get AccumulatedPrivileges for
    DirectAccessing from the owning
    element, the type, the containing
    sub-architecture, the complete architecture, and the
    connected elements;
  Get AccumulatedSafeguards for Accessed
    from the owning element, the type,
    the containing sub-architecture, and the
    complete architecture;
  Get AccumulatedPolicy for Accessed from
    similar sources;

```

Figure 13-3.  
Access control check algorithm

```

if (AccumulatedPolicy exists)
  if (AccumulatedPolicy grants access)
    return grant;
  else
    return deny;
else
  if (AccumulatedPrivileges contains
    AccumulatedSafeguards)
    return grant;
  else
    return deny;
End;

```

In order to make a decision whether to allow such access, the simplest approach is to check whether the accumulated privileges of the accessing element covers the accumulated permissions of the accessed element. However, the accessed element can choose to use a different policy, and the sources of the policy can be from the accessed element, the type of the element, the sub-architecture containing the element, and the complete architecture.

An architectural access control check algorithm is described in Figure 13-3. The algorithm first checks whether the accessing interface and the accessed interface are connected in the architecture topology. If not, the algorithm denies the architectural access. However, if they are connected, the algorithm proceeds to find the interface in the path that is nearest to the accessed interface, namely the direct accessing interface. If the accessing interface and the accessed interface are directly connected, this direct accessing interface is the same as the accessing interface. Then, the privileges of the direct accessing interface are accumulated using various contexts. Similarly, the safeguards and policies of the accessed interface are also collected. If a policy is explicitly specified by the architect, then the policy is consulted to decide whether the accumulated privileges are sufficient for the access. If there is no explicit policy, then the access is granted if the accumulated privileges contain the accumulated safeguards as a subset.

This algorithm checks architectural access control for a pair of interfaces. Extending it to the global system architecture can be achieved by enumerating each pair of interfaces and then applying the algorithm to each pair. If the global architecture contains sub-architectures, then a completely flattened architecture graph, where containers' privileges are propagated to the contained elements, is first constructed. Afterwards, the algorithm is used to check architectural access control between relevant pairs of interfaces belonging to this architecture graph.

Let us examine how the models and techniques for architectural access control can be applied to two real-world applications, one based on secure cooperation and Firefox as the other.

#### Example: Secure Cooperation

The first example of architectural access control that we consider is an application that requires secure cooperation between its participants. The software architecture of the application is expressed in the C2 architectural style. The application allows two parties to share data with each other. However, these two parties do not necessarily fully trust each other; thus, the data shared should be subject to the control of each party.

The two parties participating in this application are an insurance company and a hospital. Each of them can operate independently and display the messages they receive from their own information sources. For example, the insurance company may exchange messages about an insured person's policy status, and the hospital sends the medical history of a patient among its departments. The two parties also need to share messages so the insurance company can pay for the service the hospital provides to patients. To accomplish this, the hospital sends a message to the insurance company, including the patient's name and the service performed. After verifying the policy, the insurance company sends a message back to the hospital, authorizing paying a certain amount from a certain account. While the two parties need to exchange information, such sharing is limited to certain types of messages. Governing laws, like the United States' Health Insurance Portability and Accountability Act (HIPAA), might prohibit one party from sending certain information to the other, such that the hospital cannot send a person's full medical conditions to the insurance company. Moreover, maintaining business competitiveness also requires each party not to disclose unnecessary information, such that the insurance company would not want to send a person's auto policy information to the hospital.

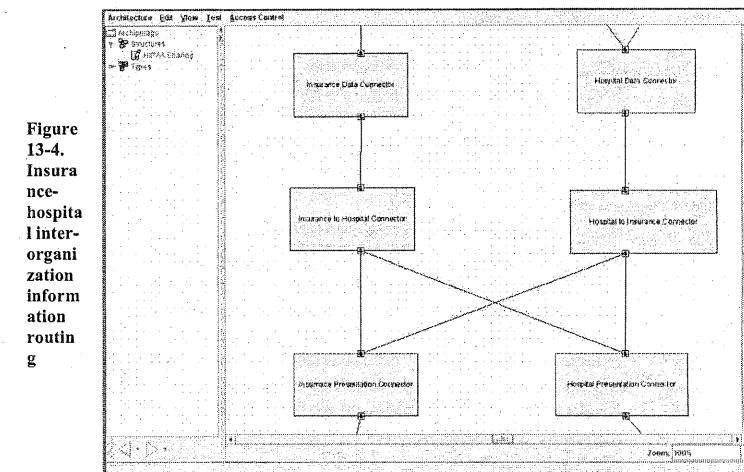


Figure 13-4 depicts the application architecture which uses a secure connector on each side that securely routes messages between the insurance company and the hospital. When the insurance to hospital connector receives a message, it inspects the message, and if the message can be delivered to both the company and the hospital, such as a payment authorization message, then the message is forwarded to both sides. Otherwise, the message is only transferred within the insurance company. The hospital to insurance connector operates in a similar fashion.

The data sharing can be controlled in a number of ways by setting different policies on the connectors. For instance, each of the connectors can be denied instantiation which will prevent any sharing to occur. Even if both connectors are instantiated, the connections with other components and connectors can still be rejected to prevent message delivery and data sharing. When the connectors are instantiated and properly connected with other elements, each of them can still use its own policy on internal message routing to control what messages can be delivered to its own side and the other side.

This architecture also promotes understanding and reuse: Only two secure connectors are used, these connectors perform a single task of secure message routing, and they can be used in other cases by adopting a different policy.

### Example: Firefox

Firefox is an open source web browser first released in November 2004. It uses three key platform technologies: XPCOM, a cross platform component model, JavaScript, the web development programming language which is also used to develop front end components of Firefox, and XPCConnect, the bidirectional connection between native XPCOM components and JavaScript objects.

#### *Trust Boundary between Chrome and Content*

When a user uses the Firefox browser to browse the web, the visible window contains two areas. The chrome, which consists of decorations of the browser window, such as the menu bar, the status bar, and the dialogs, are controlled by the browser. The browser is trusted to perform arbitrary actions to accomplish the intended task. Borrowing the chrome term that originally refers to the user interface elements, the browser's code is called the **chrome code**. Such code can perform arbitrary actions. Any installed third party extensions also become a part of the chrome code.

The other area, the content area, is contained within the browser chrome. The content area contains content coming from different sources that are not necessarily trustworthy. Some of this content may contain active code that executes JavaScript scripts. Such **content code** should not be allowed to perform arbitrary actions unconditionally and must be restricted accordingly. Otherwise, they could abuse their unlimited privileges to cause damage or harm to the users. This boundary between the chrome code and the content code is the most important trust boundary in Firefox.

Because of the architectural choice of using XPCOM, JavaScript, and XPCConnect to develop the Firefox browser and extensions, both chrome code and content code written in JavaScript can use XPCConnect to access interfaces of XPCOM components that interact with the underlying operating system services. The XPCOM components are represented as the global Components collection in JavaScript.

XPCConnect, as the connector between the possibly untrustworthy accessing code and the accessed XPCOM components, should protect the XPCOM interfaces and decide whether the access to those interfaces should be permitted.

#### *Trust Boundary between Contents from Different Origins*

Another trust boundary is between contents having different origins. The origin of content is determined by the protocol, the host name, and the port used to retrieve the content. Contents differing in either the protocol, the host name, or the port would be considered to have different origins. Users

may browse many different sites, and any page can load content from different origins. The content coming from one source should only be able to read or write content originating from the same source. This is called the *same-origin* policy. Otherwise, a malicious page from one source could use this cross domain access to retrieve or modify sensitive information from another origin, such as the password that the user uses for authentication with the other origin. This is an architectural access control process where interfaces of a content component from one origin should not be inappropriately accessed by another content component from another origin.

#### *Principals*

Since the JavaScript language does not specify how security should be handled, the Firefox JavaScript implementation defines a principal-based security infrastructure to support enforcing the trust boundaries. There are two types of principals. When a script is accessing an object, the executing script has a *subject principal* and the object being accessed has an *object principal*.

Firefox uses principals to identify code and content coming from different origins. Each unique origin is represented by a unique principal. The principal in Firefox corresponds to the Subject construct in Secure xADL. Such Subjects are used to regulate architectural access control.

#### *XPCConnect: Secure Connector*

The security manager within the XPCConnect architectural connector coordinates critical architectural operations: it regulates the access by scripts running as one principal to objects owned by another principal (if the subject principal is not the system principal, then both principals should be the same for the access to be allowed), it decides whether a native service can be created, obtained, and wrapped (one type of architectural instantiation operation), and it also arbitrates whether a URL can be loaded into a window (another type of architectural instantiation operation).

Figure 13-5 depicts the Firefox component security architecture. Interfaces of the native XPCOM components executing with the chrome role are accessible from other chrome components but should be protected from other content components. The XPCConnect connector maintains this boundary between content code and chrome code. The content components from one origin, including the containing window or frame and the DOM nodes contained within them, form a sub-architecture. Their interfaces can be manipulated by chrome components, but should be protected from content components from other origins. The XPCConnect

connector maintains this boundary of same origin and helps achieve the needed protection.

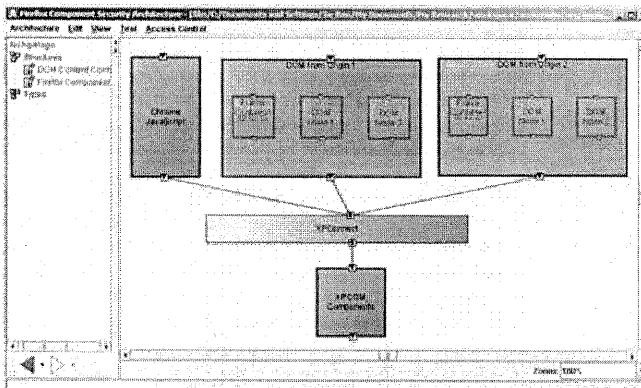


Figure 13-5.  
Firefox compo-  
nent securi-  
ty architec-  
ture

To briefly summarize this section, we first defined the access control models needed to enforce security and illustrated how they can be applied at the architecture level through the use of concepts such as *subject*, *principal*, *resource*, *privilege*, *safeguard*, and *policy*. We next demonstrated how these concepts can be incorporated into an architecture description using the Secure xADL architecture description language as an example. The resulting architecture description can be checked to verify that the architectural accesses occur only as intended. The concepts, languages and algorithms allow an architect to evaluate the security properties of alternative architectures and choose designs that suit secure requirements. We also discussed two example applications to illustrate these benefits.

In the next section, we will discuss another security notion, i.e. trust, and show how an architecture approach can be successfully used to integrate trust management within environments where participants are decentralized and make independent trust decisions in the absence of a centralized authority.

## 13.4 Trust Management

Trust Management relates to how entities establish and maintain trust relationships with each other. Trust Management plays a significant role, particularly in decentralized applications (such as the peer-to-peer

architectures discussed in Chapter 11) where entities do not have complete information about each other and the system, and thus must make local decisions autonomously. Entities must account for the possibility that other entities may be malicious and may indulge in attacks with an intention to subvert the system. In the absence of a centralized authority that can screen the entry of entities in the system, manage and coordinate the peers, and implement suitable trust mechanisms, it becomes the responsibility of each decentralized entity to adopt suitable measures to safeguard itself. Trust relationships, in such applications, help entities to gauge the trustworthiness of other entities and thus make well-informed decisions to protect themselves from potential attacks.

It is, thus, critical to choose an appropriate trust management scheme for a decentralized application. However, this by itself is not enough. For example, consider the analogy of a house, access to which is restricted through a lock on the front door. The owner may be worried that the lock may be easily picked by thieves and so may explore new kinds of locks that are harder to break; however, the owner may not realize that the windows are unsecured and can be easily penetrated. Thus, it is important to focus on both the lock as well as the windows to ensure the security of the house. Similarly, it is important to focus not only on a reliable trust management scheme but also on fortifying each entity in order to better secure entities in decentralized applications. This is possible through a software architecture approach that guides the integration of a suitable trust model within the structure of each entity and includes additional security technologies to address the pervasive concern of trust.

Our detailed focus in this section will mostly be on incorporating reputation-based trust management systems within the architecture of decentralized entities. Reputation-based trust management systems are those that use an entity's past reputation to determine its trustworthiness. However, before delving deeper into reputation-based systems, we present a brief discussion on concepts related to trust and reputation.

### 13.4.1 Trust

The concept of trust is not new to humans nor is it limited only to electronic entities. Trust is an integral part of our social existence: our interactions in society are influenced by the perceived trustworthiness of other entities. Thus, in addition to computer scientists, researchers from other fields such as sociology, history, economics, and philosophy have devoted significant attention to the issue of trust[183]. Given the fact that trust is a multi-disciplinary concept, several definitions of trust exist in the literature. However, since the discussion here is in the context of software development, we present below a definition of trust coined by Diego Gambetta that has been widely adopted by computer scientists.

Diego Gambetta [84] defines trust as *a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action.*

The above definition notes that trust is subjective and depends upon the view of the individual. In other words, whether someone can be trusted and if so, to what extent, depends upon who is trying to evaluate the trustworthiness. Thus, the perception of trustworthiness may vary from person to person.

Further, trust can be multi-dimensional and depends upon the context in which trust is being evaluated. For example, A may trust B completely when it comes to repairing electronic devices but may not trust B when it comes to repairing cars. The concept of context is thus critical since it can influence the nature of trust relationships significantly.

Gambetta also introduced the concept of using values for trust. These values may express trust in several different ways. For example, trust may be expressed as a set of continuous real values, binary values, or a set of discrete values. The representation and expression of trust relationships depends upon the application requirements. For example, an application may only need to establish and know if an entity can be trusted or not in which case binary values for trust may be used. If instead, the application requires entities to compare trustworthiness of several entities, a richer expression of trust values is required, thus, motivating the need for continuous trust values.

Trust is conditionally transitive. This means that if an entity A trusts entity B and entity B trusts entity C, it may not necessarily follow that entity A can trust entity C. There are a number of parameters that influence whether entity A can trust entity C. For example, entity A may trust entity C only if certain possibly application-specific conditions are met, or if the context of trust is the same.

#### 13.4.2 Trust Model

A trust model describes the trust relationships between entities. Realizing the immense value of managing trust relationships between entities, a number of trust models have been designed. These models are geared at different objectives and targeted at specific applications and hence embody different definitions of “trust model”. For some, it may mean just a trust algorithm and a way of combining different trust information to compute a single trust value, while for some others a trust model may also

encompass a trust-specific protocol to gather trust information from other entities. Yet others may want a trust model to also specify how and where trust data is stored.

We present a unifying definition of a trust model and identify the essential elements that constitute a trust model. We define a trust model as follows - *a trust model describes what trust information is used to establish trust relationships, how that trust information is obtained, how that trust information is combined to determine trustworthiness, and how that trust information is modified in response to personal and reported experiences.*

This definition of a trust model identifies three important components of a trust model. The first component specifies the nature of trust information used and the protocol used to gather that information. The second component dictates how the gathered information is analyzed to compute a trust value. Finally, the third component determines not only how an entity's experiences can be communicated to other entities but also how it can be incorporated back into the trust model.

#### 13.4.3 Reputation-based Systems

Related to trust is the concept of *reputation*. Abdul-Rahman and Stephen Hailes [5] define reputation as *an expectation about an individual's behavior based on information about or observations of its past behavior*. In online communities, where an individual may have little information to determine the trustworthiness of others, reputation information is typically used to determine the extent to which they can be trusted. An individual who is more reputed is generally considered to be more trustworthy.

Reputation may be determined in several ways. For example, a person may either rely on his direct experiences, or rely on the experiences of other people, or a combination of both to determine the reputation of another person. Trust management systems that use reputation to determine the trustworthiness of an entity are termed reputation-based systems. There are several applications, such as Amazon.com and eBay.com, that employ such reputation-based systems.

Reputation-based systems can be either centralized or decentralized. A decentralized reputation-based system is one where every entity directly evaluates other entities, maintains those evaluations locally, and interacts directly with other entities in order to exchange trust information. A centralized reputation-based system, on the other hand, relies on a single centralized authority to either facilitate evaluations and interactions between entities or to store relevant trust information. Amazon.com and eBay.com provide a central repository to store reputation information provided by their users while XREP, a trust model for P2P file-sharing

applications, is an example of a decentralized reputation-based system. Next, we next take a deeper look at eBay and XREP.

### eBay

eBay is an electronic marketplace where users sell and buy different kinds of goods. Sellers advertise items and buyers place bids for those items. After an auction ends, the winning bidder buys the advertised item from the seller. Both buyers and sellers rate each other after the completion of a transaction. A positive outcome results in a +1 rating and a negative outcome results in a -1 rating. These ratings form the reputation of buyers and sellers. This reputation information is stored and maintained by eBay instead of its users. eBay is, thus, not a purely decentralized reputation system. If eBay's centralized data stores were to become unavailable, eBay users would have no access to the trust information of other users.

eBay allows this trust information to be viewed through user profiles. A user can click on the profile of a buyer or seller to view their past interaction history and trust information. The profile includes the number of total interactions a user has been involved in along with his total trust score. This score, called the Feedback Score, is computed as follows: a positive rating increases the Feedback Score by 1, a negative rating decreases the Feedback Score by 1, and a neutral rating leaves the Feedback Score unaffected. A user can only affect another user's Feedback Score by one point. For example, if a user were to leave three positive ratings for another user, the Feedback Score would only increase by 1. Similarly, even if a user were to leave five negative ratings and two positive ratings, the Feedback Score would only decrease by 1. The profile also lists the total number of positive, negative and neutral ratings the user has received. Further, the profile also displays the aggregate of the most recent ratings received in the last one month, six months, and twelve months. A user viewing a profile can also choose to read all the comments written about the particular buyer or seller.

Such a system can be manipulated to defeat its purpose, of course. The case of eBay in 2000 is a classic example of a set of peers engaging in fraudulent actions [Dingledine, 2003 #2984]. A number of peers first engaged in multiple successful eBay auctions and ensured that their trust ratings went up. Once their trust ratings were sufficiently high to engage in high-value deals, these peers used their reputations to start auctions for high-priced items, received payment for those items, and then disappeared, leaving the buyers defrauded.

### XREP

XREP, proposed by Damiani et al. [49], is a trust model for decentralized peer-to-peer (P2P) file-sharing applications. P2P file-sharing applications

consist of a distributed collection of entities, also called peers, that interact and exchange resources, such as documents and media, directly with other peers in the system. A decentralized P2P file-sharing application, such as one based on Gnutella, is characterized by the absence of a centralized authority that coordinates interactions and resource-exchanges among peers. Instead, each peer directly queries its neighboring peers for files and this query is subsequently forwarded to other peers in the system. Each queried peer responds positively if it has the requested resource. Upon receiving these responses, the query originator can choose to download the resource from one of the responding peers.

While such decentralized file-sharing applications offer significant benefits, such as no single point-of-failure and increased robustness in addition to allowing users at the edge of the network to directly share files with each other, they also become a host to several attacks by malicious peers. This is because such decentralized P2P file-sharing applications are also open, implying that anyone can join and leave the system at any time without any restrictions. Peers with malicious intention may offer tampered files or may even disguise trojan horses and viruses as legitimate files and make them available for download. In the January 2004 issue of Wired magazine, an article by Kim Zetter titled "Kazaa delivers more than tunes" [307] mentions a study in January 2004 that reported that 45% of 4,778 executable files downloaded through the Kazaa file-sharing application contained malicious code like viruses and Trojan horses. When unsuspecting users download such files, they may not only harm their own computers but also unknowingly spread these malicious files to other users.

Clearly, there is a need for mechanisms that will help determine the trustworthiness of both peers and the resources offered by them. Decentralized reputation-based trust schemes offer a potential solution to this problem by using reputation to determine the trustworthiness of peers and resources. XREP is an example of such a reputation-based scheme for decentralized file-sharing applications. XREP includes a distributed polling algorithm to allow reputation values to be shared among peers, so that a peer requesting a resource can assess the reliability of both the peer and the resource offered by a peer.

The XREP distributed protocol consists of the following phases: resource searching, resource selection and vote polling, vote evaluation, best servant check, and resource downloading as illustrated in Figure 13-6. Resource searching is similar to that in Gnutella and involves a servant (i.e. a Gnutella peer) broadcasting to all its neighbors a *Query* message containing search keywords. When a servant receives a *Query* message, it responds with a *QueryHit* message. In the next phase, upon receiving *QueryHit* messages, the originator selects the best matching resource

among all possible resources offered. At this point, the originator polls other peers using a *Poll* message to enquire their opinion about the resource or the servant offering the resource. Upon receiving a *Poll* message, each peer may respond by communicating its votes on the resource and servants using a *PollReply* message. These messages help identify reliable resources from unreliable ones, and trustworthy servants from fraudulent ones.

In the third phase, the originator collects a set of votes on the queried resources and their corresponding servants. Then it begins a detailed checking process which includes verification of the authenticity of the *PollReply* messages, guarding against the effect of a group of malicious peers acting in tandem by using cluster computation, and sending *TrueVote* messages to peers that request confirmation on the votes received from them. At the end of this checking process, based on the trust votes received, the peer may decide to download a particular resource. However, since multiple servants may be offering the same resource, the peer still needs to select a reliable servant. This is done in the fourth phase where the servant with the best reputation is contacted to check the fact that it exports the resource. Upon receiving a reply from the servant, the originator finally contacts the chosen servant and requests the resource. It also updates its repositories with its opinion on the downloaded resource and the servant who offered it.

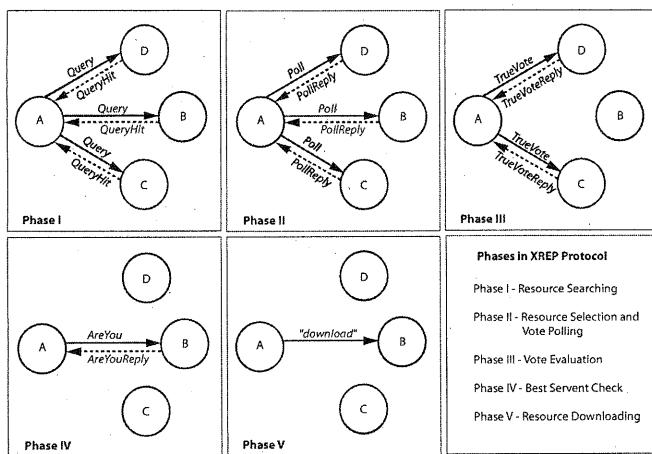


Figure 13-6. Phases in XREP. (Diagram courtesy Girish Suryanarayana)

### 13.4.4 Architectural Approach to Decentralized Trust Management

The nature of decentralized systems and their susceptibility to various types of attacks makes it critical to design such decentralized systems carefully. As mentioned previously, software architecture provides an excellent basis to reason about these trust properties and can serve to provide comprehensive guidance on how to build such systems. In particular, it provides guidance on how to design and build each decentralized entity so that it can protect itself against attacks as well as still retain its independence to make local autonomous decisions. There are three main steps involved in such an architectural approach: understanding and assessing the real threats to a system, designing countermeasures against these threats, and incorporating guidelines corresponding to these countermeasures into an architectural style.

#### Threats to decentralized systems

##### Impersonation

Malicious peers may attempt to conceal their identities by portraying themselves as other users. This may happen in order to capitalize on the pre-existing trust relationships of the identities they are impersonating and the targets of the impersonation. Therefore, the targets of the deception need the ability to detect these incidents.

##### Fraudulent Actions

It is also possible for malicious peers to act in bad faith without actively misrepresenting themselves or their relationships with others. A user can indicate that they have a particular service available even when they knowingly do not have it. Therefore, the system should attempt to minimize the effects of bad faith.

##### Misrepresentation

Malicious users may also decide to misrepresent their trust relationships with other peers in order to confuse. This deception could either intentionally inflate or deflate the malicious user's trust relationships with other peers. Peers could publish that they do not trust an individual that they know to be trustworthy. Or, they could claim that they trust a user that they know to be dishonest. Both possibilities must be taken into consideration.

##### Collusion

A group of malicious users may also join together to actively subvert the system. This group may decide to collude in order to inflate their own trust values and deflate trust values for peers that are not in the collective.

Therefore, a certain level of resistance needs to be in place to limit the effect of malicious collectives.

#### *Denial of Service*

In an open architecture, malicious peers may launch an attack on individuals or groups of peers. The primary goal of these attacks is to disable the system or make it impossible for normal operation to occur. These attacks may flood peers with well-formed or ill-formed messages. In order to compensate, the system requires the ability to contain the effects of denial of service attacks.

#### *Addition of Unknowns*

In an open architecture, the cold start situation arises: upon initialization, a peer does not know anything about anyone else on the system. Without any trust information present, there may not be enough knowledge to form relationships until a sufficient body of experience is established.

Therefore, the ability to bootstrap relationships when no prior relationships exist is essential.

#### *Deciding Whom to Trust*

In a large scale system, certain domain-specific behaviors may indicate the trustworthiness of a user. Trust relationships should generally improve when good behavior is perceived of a particular peer. Similarly, when dishonest behavior is perceived, trust relationships should be downgraded accordingly.

#### *Out-of-Band Knowledge*

Out-of-band knowledge occurs when there is data not communicated through normal channels. While trust is assigned based on visible in-band interactions, there may also exist important invisible interactions that have an impact on trust. For example, Alice could indicate in person to Bob the degree to which she trusts Carol. Bob may then want to update his system to adjust for Alice's out-of-band perception of Carol. Therefore, ensuring the consideration of out-of-band trust information is essential.

### **Measures to address these threats**

#### *Use of Authentication*

In order to prevent impersonation attacks, it is essential to use some form of authentication, so that message senders can be uniquely identified. Entities sign outgoing messages and receiving entities verify those signatures to validate the authenticity of those messages. Signature-based authentication, such as that discussed at the beginning of this chapter, also helps protect against potential repudiation attacks – attacks where an entity may falsely claim that it never sent the message.

#### *Separation of internal beliefs and externally reported information*

In a decentralized system, each entity has its own individual goals which may conflict with those of other entities. It is therefore important to model externally reported information separately from internal beliefs. This separation helps resolve conflicts between externally reported information and internal perceptions. For example, a peer may favor information it has perceived directly and believes to be accurate over information reported by others. A peer may also not want to disclose sensitive data, so it must have the ability to report information which differs from what it actually believes. ("What I've heard is ....")

#### *Making trust relationships explicit*

Without a controlling authority that governs the trust process, peers require information to make decisions whether or not to trust what they perceive. Active collaboration between peers may provide enough knowledge for peers to reach their local decisions. Thus it is important that information about trust relationships be explicit and exchangeable between peers. There is a possibility that exposing trust information may be misused by malicious peers to take advantage of certain peers; however, it should be remembered that exchanged information may not truly reflect the trust perceptions of the entities.

#### *Comparable trust*

Ideally, published trust values should be syntactically and semantically comparable - that is, equivalent representations in one implementation should have the same structure and meaning in another. If the same value has different meanings across implementations, then accurate comparisons across peers cannot be made.

#### **Corresponding guidelines to incorporate into an architectural style**

#### *Digital Identities*

Without the ability to associate identity with published information, it is a challenge to develop meaningful trust relationships. Thus, the concept of identities, both physical and digital, is necessary to facilitate meaningful relationships. However, it is important to understand the limitations of digital identities with respect to physical identities.

There may not be a one-to-one mapping between digital and physical identities as one person may utilize multiple digital identities or multiple people may share the same digital identity. Additionally, anonymous users may be present who resist digital identification. Therefore, it is not always possible to tie a digital identity to one physical individual and make accurate evaluations of a person. Instead, a critical criterion of trust relationships in decentralized applications should be the actions performed by digital identities, not by physical identities. The architectural style should therefore consider trust relationships only between digital identities.

### *Separation of Internal and External Data*

Explicit separation of internal and external data supports the separation of internal beliefs from externally reported information within a decentralized entity. Therefore, the architectural style should adopt the explicit separation of internal and external data.

### *Making Trust Visible*

Trust information received externally from entities is used within the peer architecture to make local decisions. In order to process this trust information internally across the entire architecture, trust cannot be localized to only one component. Each component responsible for making local decisions needs the ability to take advantage of this perceived trust. If the perceived trust is not visible, then accurate assessments may not be made. Therefore, the architectural style should require trust relationships to be visible to the components in the peer's architecture as well as be published externally to other peers.

### *Expression of Trust*

There has been no clear consensus in the trust literature as to which trust semantics provide the best fit for applications, therefore it is believed that indiscriminately enforcing a constraint at the architectural level to use a particular trust semantic is inappropriate. While trust values should be semantically comparable, a generic architectural style might only impose the constraint that trust values must at least be syntactically comparable. For example, this can be done by enforcing that trust values be represented numerically.

### **Resultant Architectural Style**

The principles and constraints identified above are combined to create an architectural style for decentralized trust management. In addition to these constraints, based on the common elements of trust models, four functional units of a decentralized entity are first identified. These are Communication, Information, Trust, and Application. The Communication unit handles interaction with other entities, the Information unit is responsible for persistently storing trust and application-specific information, the Trust unit is responsible for computing trustworthiness and guides trust-related decisions, and the Application unit includes application-specific functionality and is responsible for enabling local decision-making. The Communication unit does not depend upon any other units while the Information unit depends upon information received from other entities and thus depends upon interaction with them. The Trust unit depends upon the Communication and Information units and the Application builds upon all the other three units.

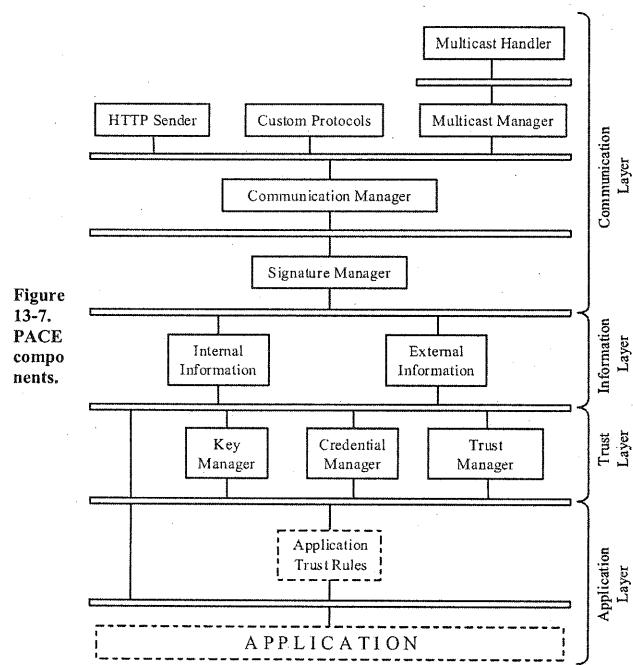
Given this interplay between the four units, it can be seen that adopting a layered architectural style enables a natural structuring of these units

according to their interdependencies as well as offers several benefits such as reusability of components that can be leveraged. Since decentralized entities are autonomous, they have the privilege of refusing to respond to requests of other entities. As a result decentralized applications typically employ asynchronous event-based communication protocols. In order to reflect this communication paradigm within the internal architecture of an entity, an event-based architectural style for the architecture of an entity is natural. Moreover, event-based architectural styles have been known to successfully facilitate loose coupling among components. This can, for instance, allow for the replacement of trust models and protocol handlers in the architecture.

C2 is one such event-based layered architectural style. As discussed in Chapter 4, C2 includes specific visibility rules – components belonging to a layer are only aware of components in layers above and are unaware of components below them. C2 thus naturally fits in with the constraints of a trust-centric architectural style. Further, C2 also has existing tool support that can be leveraged by an architectural style based on C2. Therefore, the PACE architectural style, described next, extends the C2 style.

### **PACE Architectural Style**

The PACE architectural style includes all the above-described guidelines and constraints and provides comprehensive guidance on what components must be included within the architecture of an entity and how they should interact with each other. Corresponding to the four functional units, PACE divides the architecture of a decentralized entity into four layers: Communication, Information, Trust, and Application. Each of these layers along with their components is illustrated in Figure 13-7.



The Communication layer is responsible for handling the communication with other peers in the system. It consists of three components: the Protocol Handler, Communication Manager, and Signature Manager. The Protocol Handler implements multiple network communications which are responsible for translating internal events externally. The Communication Manager instantiates the protocol handlers while the Signature Manager signs requests and verifies notifications.

To separate the internal beliefs of a peer from those received from other peers, the Information layer consists of two components: the Internal Information component that stores self-originating messages and the External Information component which stores messages received from others.

The Trust layer incorporates the components that enable trust management. This layer consists of the Key Manager (which generates the local PKI keypair), the Credential Manager (which manages the

credentials of other peers), and the Trust Manager (which computes trust values for messages received from other peers).

The Application layer encapsulates all application-specific components. The Application Trust Rules component encapsulates the rules for assigning trust values based on application-specific semantic meanings of messages, and supports different dimensions of trust relationships. The Application sub-architecture represents the local behavior of a peer. While components in the other layers can be reused across different applications, components in the Application layer are application-dependent and hence not reusable across domains. The application developer is thus expected to implement components for this layer depending upon the application's needs.

#### PACE Induced Benefits

PACE's guiding principles induce properties that act as countermeasures against threats to a decentralized system. Some of these properties are effected by the PACE architectural style and canonical implementations of its standard components; others are application specific and so involve the Application layer. We now take a look at some of the common threats and the way PACE helps address them. It should be noted that it is not mandatory for all peers participating in a decentralized system to be built in the PACE architectural style in order to function and interact with PACE-based peers. However, those peers cannot avail themselves of the benefits of the PACE style.

#### Impersonation

Impersonation refers to the threat caused by a malicious peer posing as another in order to misuse the peer's privileges or reputation. PACE addresses this threat through the use of digital signatures and message authentication. Since all external communication in the PACE architecture is constrained to the Communication layer, it offers a single point where impersonation can be detected. The deception of a malicious peer that tries to impersonate a user without the correct private key or does not digitally sign the message, can be easily detected by verifying signatures. Additionally, if a private key has been compromised, a revocation for that key can be transmitted. PACE components can then refuse to assign trust values to revoked public keys.

#### Fraudulent Actions

Malicious peers may engage in fraudulent behavior including advertising false resources or services and not fulfilling commitments. Since PACE is designed for open, decentralized architectures, there is little that can be done to prevent the entry of malicious peers. However, malicious actions can be detected by the user or through the Application layer. Explicit

warnings can then be issued concerning those malicious peers which may help others in their evaluations of these peers.

#### *Misrepresenting Trust*

A malicious peer may misrepresent its trust with another in order to positively or negatively influence opinion of a specific peer. Since PACE facilitates explicit communication of comparable trust values, a peer can incorporate trust relationships of others. By using a transitive trust model in the trust manager, if Alice publishes that she distrusts Bob, then Carol can use that information to determine if she should trust Bob's published trust relationships.

#### *Collusion*

Collusion refers to the threat caused by a group of malicious peers that work in concert to actively subvert the system. It is thus of greater concern than a single peer misrepresenting trust. It has been proven that explicitly signed communication between peers can overcome a malicious collective in a distributed setting. Adapting and combining these results with efficient schemes to identify non-cooperative groups in a decentralized setting (such as in NICE [163]) with PACE's ability to detect impersonation allows collusion to be effectively addressed.

#### *Denial of Service*

Malicious peers may also launch attacks against peers by flooding them with well-formed or ill-formed messages. The separation of the Communication layer allows isolation and response of the effects of such denial of service attacks. Incorrectly-formed messages can be disposed of by the protocol handlers. The communication manager can also compensate for well-formed message floods by introducing rate limiting or interacting with neighboring firewalls to prevent further flooding.

#### *Addition of Unknowns*

When the system is first initialized, there can be a cold start problem because there are no existing trust relationships. Even though a peer may not have previously interacted with another peer or a message may be known to be forged, PACE's Application layer can still receive these events. Without enough information to make an evaluation, the message will not be assigned a trust value by the trust manager. However, the user can still make the final decision to trust the contents of the message based on out-of-band knowledge that is not captured explicitly.

#### *Deciding Whom To Trust*

In a large-scale system, certain domain-specific behaviors may indicate the user's trustworthiness. Trust relationships should generally improve when good behavior is perceived of a particular peer and vice versa. In PACE, the application trust rules component allows for automated identification of application-dependent patterns. The detection of good or

bad behavior by this component can cause the trust level of the corresponding peer to be increased or decreased respectively along a particular trust dimension.

#### *Out-of-Band Knowledge*

It is essential to ensure that out-of-band information is also considered in establishing trust relationships. While PACE confines all electronic communication to the Communication layer, out-of-band trust information can originate as requests from the user through the Application layer.

#### **Building a PACE-based trust-enabled decentralized file-sharing application**

In this section, we present a walk-through of how PACE can be used to design and construct applications. Specifically, let us explore how the PACE architectural style can be used to guide the construction of a trust-enabled decentralized file-sharing application. Since the XREP trust model for file-sharing applications was presented above, it will be used as the candidate trust model for integration within the PACE style.

The first step in designing an appropriate architecture for each file-sharing entity is to identify the components in the four layers. Since the PACE architectural style already specifies components for the Communication, Information, and Trust layers, the main task here is to identify the components of the Application layer. For the file-sharing application, the Application layer can be decomposed, for example, into eleven different components organized into three sub-layers as shown in Figure 13-8.

The top sub-layer contains only the Application Trust Rules component while the bottom sub-layer includes the user interface. The middle sub-layer consists of the following six components: Library, Search Manager, Poll Manager, File Exchanger, Evaluator, and Preferences. The Library component maintains the list of files that have been downloaded and that can be shared with other peers. However, these files are persistently stored in the Internal Information. The Search Manager component is responsible for issuing *Query*, *Poll*, and *TrueVote* messages and displaying received responses to those messages through the user interface.

The Poll Manager component responds to *Poll* messages by sending *PollReply* messages. The File Exchanger component is responsible for uploading and downloading files, displaying uploaded and downloaded files to the user interface, saving downloaded files to the Internal Information storage, and deleting files from the Internal Information. The Evaluator component is responsible for checking the authenticity of *PollReply* messages and analyzing peer votes received about resources. The Preferences component manages login information for the user and enables the user to specify preferences including whether to automatically connect to the P2P network, the number of hops, the number of

permissible uploads and downloads, and the destination for the library folder.

Once the components of the Application layer are identified, it is important to determine the interactions between the components in order to identify the relevant request and notification messages that traverse up and down the architecture. This includes modeling the different kinds of trust messages exchanged between peers as dictated by the XREP trust model so the relevant components can appropriately react to them.

In the next step, components belonging to each layer must be appropriately implemented. If existing implementations for any of these components exist, the application developer can choose to reuse them as long as the PACE style is not violated; else, totally new implementations for the components may be required. Since PACE prototypes in other application domains already exist, it is possible to reuse all components from the Communication, Information, and Trust layers without any modifications. The only exception would be the Trust Manager component which will need to be modified to enable the evaluation of poll results within each XREP-based file-sharing peer.

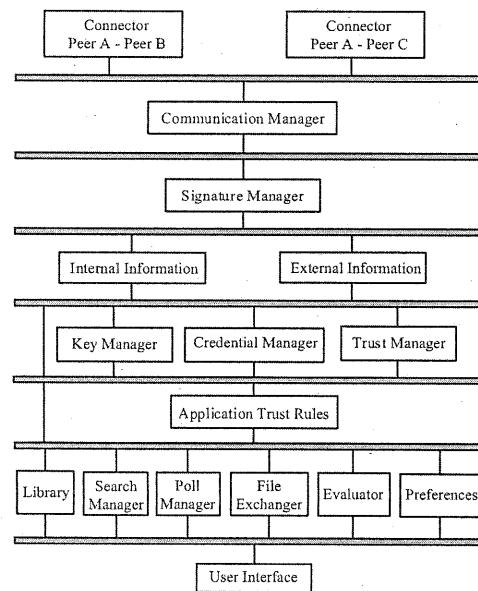


Figure 13-8.  
XREP-based  
architec-  
ture  
of file-  
sharin  
g peer.

#### The Business Case

Finally, the above-described architecture of a file-sharing peer may be described in a suitable architecture description language such as xADL. The Archstudio tool suite can be used to both describe the architecture as well as instantiate it. Each instantiation corresponds to a particular peer; thus, the same architectural description may be instantiated repeatedly to create multiple trust-enabled file-sharing peers. The resulting application can then be subjected to threat scenarios to evaluate whether XREP-enabled peers built in the PACE style can successfully counter the threats typical to file-sharing applications.

## 13.5 End Matter: Trade-offs

This chapter has presented principles, concepts, and techniques relevant to the design and construction of secure software systems. However, making a system secure may mean compromising other non-functional requirements. For example, enforcing secure interactions may make the architecture less flexible. Specifically, preventing a component from interacting with unknown components may discourage security attacks, but also implies that the capabilities offered by the unknown components cannot be leveraged.

Another example is the use of SPKI (Standard Public Key Infrastructure) for digitally authenticating messages. This mechanism involves signing transmitted messages with keys and verifying the signatures at the receiving end. Moreover, message content may be encrypted at the sending end and be decrypted at the receiving end to ensure confidentiality of message content. Algorithms used for authentication and encryption are known to be computationally intensive and thus the use of these algorithms may affect the performance of an application.

A third example relates to the trade-off between security and usability. If the security mechanism in a software system requires a user to perform cumbersome or repetitive actions (for instance, by showing redundant or unnecessary dialog prompts repeatedly), the user may choose to completely turn off the security mechanism. These examples illustrate the importance of properly considering these various kinds of trade-offs since they can affect the usefulness of a security mechanism. It is, therefore, critical for software architects and application developers to apply careful thought and consideration while designing and constructing secure software systems.

In a television advertisement for a motor oil additive, auto racing legend Andy Granatelli said “You can pay me now, or you’ll pay me later” – referring to the benefits of regular engine maintenance. The implication

was that failure to tend to the preventive needs of an engine in a timely manner could lead to expensive, if not catastrophic, failure later on. So it is with software security.

As with other software qualities, it is far more cost effective, and technically easier, to plan for and design in security from a project's outset, rather than waiting until a security breach either lands a company unfavorably in the public eye or causes a significant financial loss. Moreover an architecture-based approach focuses on a comprehensive analysis and solution strategy, not a "plug-this-leak and wait for the next disaster" reactive response.

The serendipity that accompanies architectural design for security and trust is that the discipline of analyzing a design and introducing security-focused separations and mechanisms at the outset can yield a clean design able to accommodate other, non-security focused, demands for change that arise over time.

Trust management for open, decentralized systems will continue to rise in importance as web services and other forms of open commerce increase in adoption. As the main text of this chapter has shown the techniques available have numerous limitations. These limitations are no different than those that have always existed in business, long before the advent of electronic commerce. Should you trust another vendor? Will your invoice be paid? How do you know? The legal remedies that society provides, the out-of-band communication people depend upon – these can apply in e-commerce as well. The increased difficulty, and hence the need for trust management techniques such as those described here, arises from the speed with which transactions – both legitimate and fraudulent – can take place.

## 13.6 Review Questions

1. What is security? What are the properties that a software system must exhibit in order to be called secure?
2. List and briefly describe each design principle explained in this chapter.
3. What challenges to security are introduced by decentralized applications? What is trust management?

## 13.7 Exercises

28. Identify and describe any trade-offs between the design principles explained in the chapter.
  29. What are the security benefits and the security risks associated with the following architectural styles from Chapter 4?
    - a. Pipe-and-filter
    - b. Blackboard
    - c. Event-based
    - d. C2
- In your answer consider how malicious actions in one component can or cannot affect the actions of other components.
30. Choose any software application, like Firefox, and use UML sequence diagrams to show how the security mechanisms within the application operate.
  31. Describe at least two applications, other than on-line auctions and file sharing, where trust or reputation management may prove useful, and explain the rationale for your choices.
  32. Evaluate whether the PACE architectural style could be used to build the participants in the above applications.
  33. Study the architecture of Internet Explorer 7 and evaluate whether IE 7 has any architectural security deficiencies. If so, how can these vulnerabilities be addressed? Use xACML and Secure xADL to propose a more secure architecture for IE 7.

## 13.8 Further Reading

An excellent introduction to the field of computer security is given by Bruce Schneier in [252]. This highly readable book explores the interplay of technical and non-technical issues in achieving system security. Matt Bishop's text [20] provides details of the technologies involved. Pfleeger and Pfleeger's book [228] is another comprehensive reference.

Research frontiers for software engineering for security are presented in Devanbu and Stubblebine's "roadmap" paper [60] from the 2000 International Conference on Software Engineering.

Further details on the PACE architectural style can be found in [266-268]. Further details on the connector-centric approach to security are available in [242, 243].

More recently, new results have been presented at the International Workshop on Software Engineering for Secure Systems, beginning with the 2005 workshop.

## CHAPTER 14

## 14 Architectural Adaptation

Few applications are designed, built, used, and ultimately discarded without undergoing change. Change is endemic to software: both the perceived and actual malleability of the medium coupled with the ease of altering code induces everyone associated with an application to initiate changes. Users change their minds about what they want, and hence what they require of an application. Designers seek to improve their designs with respect to performance, or appearance, or some other property. The application's usage environment can change. Whatever the reason, software developers are faced with the challenges of coping with the need to modify an application. We group all of these types of changes under the term *adaptation*: modification of a software system to satisfy new requirements and changing circumstances.

This chapter does not aspire to present techniques for dealing with all possible types of adaptation at all levels of granularity and abstraction – to do so would require a book of its own. Consistent with the focus of the book, our discussion is centered on facilitating change in the context of software architectures: we focus on adaptation to a system's principal design decisions – its architecture – and on changes that proceed from a strong architectural foundation. We consider processes for effecting change which are conceptualized in terms of the system's architecture. We show the value and role of explicit architectural models in supporting and effecting adaptation. We also consider one of the more difficult types of change: modifying applications “on the fly,” showing how this can be achieved using an architecture- and connector-centric approach.

The goals of the chapter are to:

- Characterize adaptation, showing what changes, why, and who the players are;
- Characterize the central role software architecture plays in system adaptation;
- Present techniques for effectively supporting adaptation, based on an architecture-centric perspective.

## Outline of Chapter 14

This chapter will reveal the particular power of connectors in supporting adaptation, especially in those situations where the connectors remain first-class entities in the implementation and where communication is event-based. Highly dynamic applications are possible in such situations and offer the opportunity for creating novel, flexible, highly adaptable applications.

14. Architectural Adaptation
14.1 Concepts of Architecture-centric Adaptation
14.1.1 Sources and Motivations for Change
14.1.2 Shearing Layers
14.1.3 Structural Elements Subject to Change
14.1.4 Change Agents and Context
14.1.5 Architecture: the Central Abstraction
14.2 A Conceptual Framework for Architectural Adaptation
14.3 Techniques for Supporting Architecture-centric Change
14.3.1 Basic Techniques Corresponding to Activities of the Conceptual Framework
14.3.2 Architectures/Styles that Support Adaptation
14.3.3 The Special Problems of On-the-fly and Autonomous Adaptation
14.4 End Matter
14.5 Review Questions
14.6 Exercises
14.7 Further Reading

### 14.1 Concepts of Architecture-centric Adaptation

#### 14.1.1 Sources and Motivations for Change

Several motivations for change are familiar to developers. Perhaps the most common is *corrective change*, where the application is “adapted” to conform to the existing requirements. Put in other words, bringing the descriptive architecture into conformance with the prescriptive architecture. Put most simply, bug fixing. Whether bug fixing is easy or highly disruptive, however, may depend on the root cause of an error: did the observed problem with the application stem from a small, localized error in the code, or result from a profound mistake made at the highest level of system structure? Understanding the root cause is essential for determining how to effect the fix; attempting to patch a deep problem with localized change is usually ineffectual.

A second common motivation for change is *modification to the functional requirements* for a system – new features are needed, existing ones modified, perhaps some must be removed. Rather than thinking that the

existence of such needs for change reflect an inadequate system planning or analysis process, functional change requests often proceed from success with the existing application. Once applications are in use they inspire users to think of their task in new ways, leading to new ideas for what might be accomplished. Applications in use may change the usage context, or the usage context may change for extrinsic reasons. Whatever the cause, feature change requests typically represent changes to the application's architecture.

A third motivation for change is the requirement to satisfy *new or changed non-functional system properties*. Such properties include security, performance, scale, and so on, as discussed in Chapters 12 and 13. New non-functional properties may induce profound changes to a system's architecture. One example is the World Wide Web. Prior to 1994 the Web's governing protocol was HTTP/1.0, a point-to-point protocol with no provision for proxies or caching. The change to HTTP/1.1 was accomplished by the adoption of a new architectural style for the Web (viz., REST), enabling the web to scale from thousands of servers and tens of thousands of clients, to many millions of each. Similarly, as security attacks on Microsoft's IIS web server increased, a significant redesign was required to meet the new threats. Another non-functional property that may cause significant architectural change is "better organization" – restructuring an application in *anticipation* of future change requests. For instance, a new middleware platform (i.e. connector technology) may be put in place as a pro-active step towards supporting potential future modifications.

A fourth common motivation for system adaptation is the need to conform to a *changed operating environment*. In this situation the application's functions are not altered, nor its non-functional properties, but the application's structure must be adapted to run, for example, on new hardware or to accommodate changes in interfaces to external systems.

More obviously germane to the software architect are motivations for change that *arise from product line forces*. Strictly speaking such changes can be classified under one of the preceding types of change, but such classification would obscure the insights.

The first of these product line motivations is the desire to *create a new variant* within a product line. The notion here is that the architects have previously identified a "branch point" within a product line architecture, and that with respect to that branch point a new variant is identified. For example, in consumer electronics, a branch point within the design for integrated television systems is the interface to a high-capacity storage/replay subsystem – a hard disk, a DVD recorder/player, or a tape system perhaps. If it becomes desirable to interface with a different

technology, perhaps Blu-ray, a new variant at that branch point is created. In our long-running example of the lunar lander video game, a new variant might be based upon the wish to utilize a new wireless joy-stick for controlling the lander, or to incorporate a new 3-D graphics engine having improved performance.

Another of the product line motivations is *creation of a new branch point*, thereby identifying a new opportunity for product marketplace segmentation. For instance, an electronics manufacturer may decide to adapt the design of their television products to enable them to work with home security systems, perhaps by using picture-in-picture technology to allow continuous display of surveillance camera data while watching broadcast TV. The existence of many types of external security systems implies many possible variants within this branch point; other variants are implied by the many ways of integrating surveillance information into the television display environment. New branch points in the lunar lander design might focus on multi-player environments or on extensibility to allow missions to other solar system objects.

Yet another product line motivation comes from the desire to *merge product (sub-)lines*, thereby rationalizing their architectures. A successful effort of this type will yield a common product line architecture without requiring the complete creation of a new architecture. The goal is, ostensibly, to preserve as much as possible from the contributing architectures.

One type of adaptation that will be discussed later in this chapter is "on the fly" adaptation. The difficulty of supporting such change is typically greater than for non-real time adaptation, so a few words are needed here to motivate its consideration. A simple but perhaps extreme example motivating this type of change comes from planetary exploration. The Cassini/Huygens spacecraft were launched from Cape Canaveral in October 1997; it did not reach its intended destination, Saturn, until July 2004. During transit to Saturn the on-board software systems were upgraded several times. As the Cassini website<sup>14</sup> puts it, "This development phase will never really be complete, since new command sequences are continually being created throughout Cassini's operation. New flight software will also be developed and loaded aboard the spacecraft periodically, to run in the Command Data Subsystem, Attitude and Articulation Control Subsystem, as well as in the physical science instruments onboard." As a *system* it is clear that Cassini could not be "stopped" and reloaded with the new software; rather the updates must take place while the system is in continuous operation.

<sup>14</sup> <http://saturn.jpl.nasa.gov/mission/index.cfm>

**Spacecraft software updates:**

The updating of spacecraft software while in spaceflight is an extreme case of adaptation-on-the-fly. The needs for updating reflect many sources, from new directions or priorities for a mission based upon recently discovered phenomena to bug fixes. Another source is time pressure and astrophysics: because of the relative orientation of the planets it may be essential to launch an exploration mission in a fairly narrow time frame. If the mission software is not ready by the time of launch then a workable strategy is to launch with a skeletal system and then upgrade while en route to the mission's destination.

All of these factors have arisen in the Cassini mission to Saturn. Needless to say the stakes are high in on-flight software updates, hence a very conservative, patch-oriented, update strategy is applied. A few documents are available on-line which describe the processes involved, such as <http://www.aiaa.org/Spaceops2004Archive/downloads/papers/SPACE2004sp-template00339F.pdf>

A more prosaic example is the extension of web browser functionality. If when surfing the web a resource is encountered that requires a particular type of display software (such as for a new type of audio encoding, perhaps), the browser will need to be extended. If the browser requires the user to download the new extension, perform some installation steps, and then restart the browser – or worse yet, the computer – before being able to continue, the user is inconvenienced. After restart the user will have to re-navigate to the resource which demanded the extension in the first place. A more pleasant strategy, from the user's perspective, is to support the download and installation of the new software (i.e., adaptation of the browser) *dynamically*, so that the user may continue usage in an uninterrupted manner<sup>15</sup>.

Motivations for supporting on-line (dynamic) change thus include:

- Non-stop applications: ones in which the software cannot be stopped because the “application” cannot be stopped – the services of the software are continually required or safety critical.
- Maintaining user or application state: stopping the software would cause the user to lose (mental) context or because saving

<sup>15</sup> Strictly speaking, any browser that supports Javascript is dynamically adaptable. Whenever Javascript is downloaded from a website and executed in the browser the user is taking advantage of dynamic extensibility. Most contemporary browsers are so good at this that the experience is completely transparent to the user.

and/or recreating the software’s application state would be difficult or costly.

- Re-installation difficulty: applications with complex installation properties, such as software embedded in an automobile.

Finally, all software adaptation is motivated by *observation and analysis*. While perhaps this is an obvious point, the role of observation and analysis is critical in the process of supporting software adaptation, and will be discussed later in the chapter. The behavior and properties of the extant system are observed and compared with, e.g., goals and objectives for the system, and to the extent that analysis reveals a discrepancy, adaptation activities are initiated.

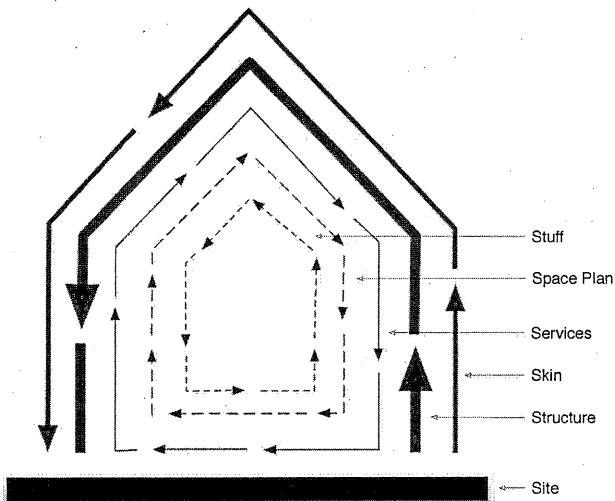
### 14.1.2 Shearing Layers

Before going further in consideration of the adaptation of software systems it is worth a moment to consider change in physical, building architecture. Stewart Brand's insightful book, *How Buildings Learn – What happens after they're built* [27], examines how, and why, buildings change over time. We have all seen this process first hand, of course: we rearrange the furniture in our offices and homes, we install new cabling in our homes to accommodate new audio systems, we install new windows to remove drafts and make a building more energy-efficient. On infrequent occasions we remodel our homes, adding new space or reconfiguring existing space. On very rare occasions we might even see a house physically moved – for instance if it is of historical significance but lies in the way of a new civic development.

Brand categorizes the types of change that can be made to a building in terms of “shearing layers”. Building upon earlier work by Frank Duffy, six layers are enunciated:

- “Site. This is the geographical setting, the urban location, and the legally defined lot, whose boundaries and context outlast generations of ephemeral buildings.”
- “Structure. The foundation and load-bearing elements are perilous and expensive to change, so people don’t. These *are* the building.”
- “Skin. Exterior surfaces now change every 20 year or so, to keep up with fashion or technology, or for wholesale repair.”
- “Services. These are the working guts of a building: communications wiring, electrical wiring, plumbing, sprinkler systems, ...”
- “Space Plan. The interior layout – where walls, ceilings, floors, and doors go.”
- “Stuff. Chairs, desks, phones, pictures, kitchen appliances, lamps, hair brushes; all the things that twitch around daily to monthly.”

These are illustrated in Figure 14-1, with the arrangement of the layers in the diagram corresponding to where, approximately, the layers appear in a physical structure.<sup>16</sup>



**Figure 14-1. Shearing Layers of Change**  
(adapted from Stewart Brand's "How Buildings Learn" [27])

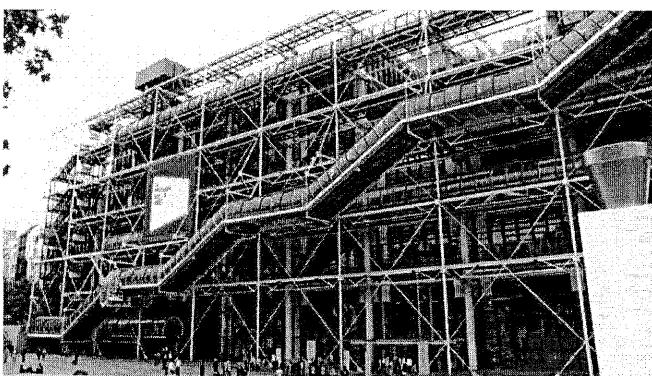
Software is like this too. Though software is intrinsically more malleable, the constraints and dependencies that we impose during the process of design and implementation make it behave much like a building. As we have seen, any software system has an architecture, which determines its "load bearing elements." It has a "site" in its installation, i.e. the usage context, whether it be a home business, a research laboratory, or a bank. Similarly, software has a "skin" with its user interfaces; further analogies can be found for the other layers. The difficult thing about software however, is that we cannot examine a software system by looking at the source code and readily distinguish one of the system's load-bearing

<sup>16</sup> N.B. Layers, as used by Brand and shown in this figure do not correspond exactly to layers as used in software. In particular the relative juxtaposition of layers in a software system, such as found in the layered style of Chapter 4, differs from the ordering of the shearing layers. As shown in this diagram, for instance, the relatively immutable structure layer is adjacent to the relatively mutable skin.

elements from a mere incidental – an item as incidental as a hair brush is in a home.

One value of Brand's observations is the categorization of types of change according to the nature and cost of making a change within those dimensions. Put another way, our understanding of building layers, either as sophisticated housing developers or simply as "occupants," informs us regarding what can be changed, how quickly, and roughly for what cost. For instance, as Brand noted, changes to a load-bearing element of a building – such as a steel girder – are just not done; to do so would likely endanger the structural integrity of the building. If we could make a similar categorization for software, one that would allow us to dependably identify the load-bearing elements of an application, it would help us understand the necessary techniques to effect a given change, and allow us to effectively estimate the time and cost to achieve the goals. Our intuition as to understanding the costs, difficulty, and time to make changes in any of these aspects to a building is pretty good, due at least in part to our long experience with buildings and their visible, material nature. Unfortunately we do not usually have that kind of intuition with software, for we often cannot associate a change request with a particular type of layer in the software.

One of Brand's objectives in identifying shearing layers with their different properties is that design guidance is provided thereby. Recognizing that the layers change at different rates, change is facilitated by limiting the coupling between the parts of a building that correspond to different shearing layers. (A simple example admonition that comes from this is "Don't inextricably associate the appearance of a building with its services" – an admonition famously contravened by Paris's Pompidou Center, as illustrated in Figure 14-2. By making the services – such as escalators – part of the skin, changing one demands changing the other. Maintenance costs for the services now must also include costs for maintaining their very public appearance.)



**Figure 14-2.** The Pompidou Center: A good lesson in why appearance should not be inextricably linked with services. Photo: RNT.

These layer notions can be applied to software. In particular, the observation of layers and the admonition to decouple them is consistent with David Parnas's dictum that software engineers should "design for change". The layer concept goes beyond that simple platitude, however, to suggest specific ways of assessing whether a proposed connection between two elements of a system is appropriate or not. Are the elements proposed for connection in separate layers? In layers that are widely separated? Is the proposed connection one that maintains the essential aspects of independence for those layers?

In Brand's analysis structure plays a somewhat distinguished role. Its relative immutability in building architecture means that it must be understood well, for it provides the bounds to the types of changes that can be applied. In the case of software, with its relative mutability, we have the opportunity for accommodating a great range of change – but only under certain conditions. We can achieve effective adaptation if we make the structure of software explicit (i.e. the system's architectural configuration of components and connectors), and provide ways for manipulating that structure. At a minimum, understanding a software system's architecture enables us to assess the potential for future changes.

Finally, Brand makes a trenchant observation about building architectures that provides key insight into software adaptation: "Because of the different rates of change of its components, a building is always tearing itself apart." As introduced in Chapter 3, a concern with software change is "architectural erosion", the regressive deviance of an application from its original intended architecture resulting from successive changes. If a programmer modifies an application based only upon local knowledge of the source code, it can be quite difficult to determine if the changes made

cut across the software's shearing layers. Put another way, the changes to code may not respect the principal design decisions that govern the application. To the extent that the boundaries are ignored while making changes, the structure is degraded. The preventative strategy for avoiding architectural erosion of this type is to base change decisions not on local analysis of the code, but on the basis of understanding and modifying the architecture, and then flowing those changes down into the relevant code, a theme we explore below.

### 14.1.3 Structural Elements Subject to Change

Any of a system's structural elements, its components, connectors, and their configuration, may be the focus of adaptation. The particular characteristics of these elements as found in a specific system will significantly determine the difficulty of accommodating change and the techniques useful for achieving it.

#### Components

Some changes may be confined to a component's interior: its interface to the outside world remains fixed, but, perhaps to achieve a particular non-functional property, the component's interior must be altered. A component's performance may be improved, for example, by a change to the algorithm that it uses internally. In many cases, however, adaptation to meet modified functional properties entails changing a component's interface.

Beyond this simple dichotomy a component may possess capabilities that facilitate its adaptation, or its role in the adaptation of the larger architecture within which it resides.

First among these capabilities is knowledge of self and exposure of this knowledge to external entities. A component may be built such that its own specifications are explicit and included within the component. A straightforward form and use of such specifications are as run-time assertions which validate that incoming parameters satisfy the assumptions upon which the component's design depends. In a verified, static (i.e. non-adaptive) world such run-time assertion checking may well be considered wasteful, but in an uncertain, adaptive world such checking may be a useful adjunct in maintaining a robust application. A less obvious use of such assertions is in gathering information that may motivate adaptations. Assertions may repeatedly detect violation of input assumptions. If a component retains a history of such violations and exposes that history to a monitoring agent, that information may guide the architect in identifying ways in which the architecture needs to be changed. More generally a component may make its full specifications available for inspection by external entities. Such a capability enables dynamic selection of components to achieve system goals and hence is

strongly supportive of adaptation. While not supported in all programming languages, component reflection is supported in Java.

Second is (self-)knowledge of the component's role in the larger architecture. For instance, a component could be built to monitor the behavior of other components in an architecture and to change its behavior depending upon the failure of an external component. A component may be able to query whether other components exist in an architecture that could be used to obtain an equivalent service. Similarly, if a component monitors its own behavior and realizes, for example, that it is not performing fast enough to satisfy its client components, it could request an external agent to perform some load-leveling or other remedial activity.

Third is the ability to proactively engage other elements of a system in order to adapt. Continuing the previous example, rather than asking an external agent to reduce the load, a component might query whether external (sub-) components are available which could be used within the component to enable it to improve its own performance. While such a scenario is currently pretty far-fetched, such a capability is only a natural progression from components which are not self-aware and not reflective, to components which are reflective but passive, to components which are not only reflective but (pro-)active in supporting system adaptation.

The capabilities listed above prefigure the general adaptation techniques discussed later in this chapter. The common theme is explicit knowledge and representation of a component's specifications and knowledge of its role within the wider architecture.

#### *Component Interfaces*

Changes to component interfaces are often inevitable when modifying functionality. Changing a component's interface, however, requires changes to the interface's clients as well: the input and output parameters must match at both ends of the interaction. Many client components may not be "interested" in the new functionality represented by the new interface, yet must be modified nonetheless.

This undesirable "ripple effect" of change has motivated creation of techniques for mitigating such impacts. A popular technique is the creation of adaptors, whereby components wanting to use the original interface invoke an adaptor component which then passes along the call to the new interface, as illustrated in Figure 14-3. A client needing the new interface calls the modified component directly. Use of a technique such as this clearly has architectural implications: new components are introduced, tracing interactions to understand system functioning becomes more involved. Subsequent changes to one of the previously unmodified methods becomes even more complex: should yet-another-adaptor be

introduced? Should the method be changed in the root component and in all the previously created adaptors? Suffice it to say for now that "local fixes" that attempt to mitigate changes to component interfaces can have serious repercussions; the architect is wise to consider, in advance, a range of techniques for accommodating change, as discussed later in this chapter.

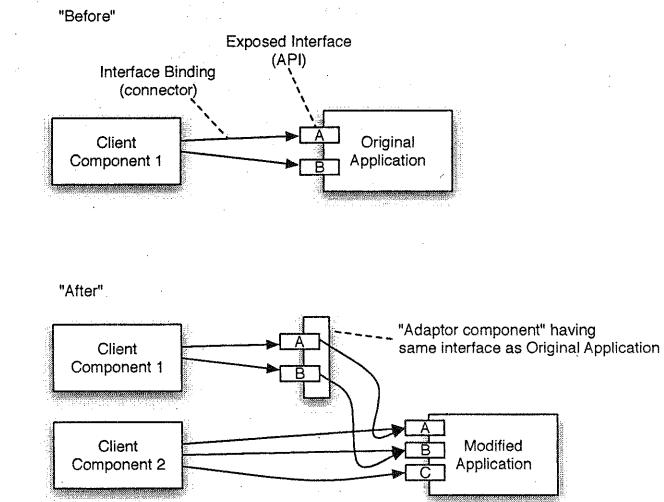


Figure 14-3. Use of adaptor components to preserve interfaces

#### *Connectors*

Just as components may be required to change, so may connectors, and depending on the type of change, the architectural implications may be profound or may be negligible, similarly for the resulting changes in the implementation. Typically changes to connectors are motivated by the desire to achieve altered non-functional properties, such as distribution of components, heightened independence of sub-architectures in the face of potential failures, increased performance, and so on.

Changes to connectors may be along any of the dimensions of connector design discussed in detail in Chapter 5. As the latter part of this chapter will show, choice of connector type is a major determinant of the effort involved in supporting architectural evolution. Roughly speaking, the more powerful the connector the easier architectural change. Connectors that remain explicit in the implementation code and which support very strong decoupling between components (such as those connectors

supporting event-based communication) are superior for supporting adaptation.

### Configurations

Changes to the configuration of components and connectors, that is, how they are arranged and linked to one another, represents fundamental change to a system's architecture. Such a change may occur at any level of design abstraction, and may be motivated by the need to meet new functional requirements or to achieve new non-functional properties. For instance, a common, large-scale configuration change is to move from a custom business-to-business application model to an open, service-oriented architecture. The custom application may enable two businesses to communicate and transact business very efficiently, but a move to an open, service-oriented architecture may allow each party to more easily add new functionality, or support interactions with other business partners. Many of the core components may remain unchanged, but the way the components interact with each other and the connectors through which they communicate may be profoundly altered.

Effectively supporting such a modification requires working from an explicit model of the architecture. Many dependencies between components will exist, and the architectural model is the basis for managing and preserving such relationships. Most importantly, the constraints that governed creation of the initial architecture must be maintained if the architecture is to retain the same style. If maintaining the governing style constraints is not possible then deliberative analysis should take place to determine an appropriate style for the new application. The move from custom business-to-business applications to service oriented architectures is precisely such a change: the fundamental architectural style of the application is altered.

The architectural model will need to manage deployment characteristics too, as basic component-connector relationships, in keeping with the discussion of Chapter 10.

#### 14.1.4 Change Agents and Context

Techniques for effecting change are determined not only by what is ultimately changed, as discussed above, but also by the *context* for the change and the character of the *agent(s)* performing the change. Important aspects of the context for change include:

- the factors behind the change motivation: how a system is observed and what analysis can be performed on those observations;

- the timing of the change: when in the development/deployment/use timeline the change occurs.

The agents for achieving change include both people and software.

Important attributes of the change agents include:

- the location of the agent with respect to the system being changed;
- the knowledge possessed by the change agent about the system, whether complete or partial;
- the degree of freedom possessed by the change agent.

Each of the above items are considered in the following paragraphs.

### Motivations, Observations, and Analysis

Several types of motivation for change were discussed at the beginning of the chapter. Depending on what particular motivation is at work different problems and opportunities for dealing with the change arise. All motivations spring from a combination of some observation about a system with analysis of those observations. For example, a system may not perform some newly desired function (as determined by comparing its current behavior to the newly sought behavior), or it may need to be fixed (as determined by comparing its current behavior to the original specification). The key issue is where the observations about a system originate.

Of course some observations may just be the engineer reviewing the system's architecture. More likely is the situation where a user, or some external agent, observes the run-time behavior of the application. To the extent that these observations are tied or related to information about the architecture of the application, the adaptation task is eased. If the only observations are those which come from seeing an application's external functional behavior, then determining the related structure is a task akin to debugging: the offending behavior has to be (possibly laboriously) examined to see what parts of the application are responsible. If the application has, or can have, probes included within it designed to assist the analyst in determining which internal elements are relevant, then the adaptation can proceed more quickly. Every beginning programmer is familiar with this technique in its simplest form: the inclusion of dozens of "println" functions, to repeatedly indicate where the program is executing, and what values particular variables have.

As architectures become more complex the beginning programmer's print line technique becomes inadequate. The concept, though, is still valuable. Monitors of the architecture can be included in a system (typically in the connectors) to enable high-quality monitoring of the behavior. The more precise the information and the analysis based on that information, the better the change can be planned and managed. In extreme cases the absence of a good technique for identifying the components responsible

for a particular behavior may cause an engineer to replace an entire subsystem. With good information, however, a much more localized change may suffice. We return to the topic of embedded probes in Section 14.3.1 below.

### Timing

The positioning of change within a project's timeline greatly affects the techniques available for accommodating the change. In short and unsurprisingly, the earlier the better. Rather than just repeating the old maxim that fixing problems in requirements is substantially cheaper than fixing them in code, we expand the timeline to include system deployment and system use, for indeed some applications may need to be changed *in situ*, on the fly. A notional graph showing the relationship between cost and timing is found in Figure 14-4.

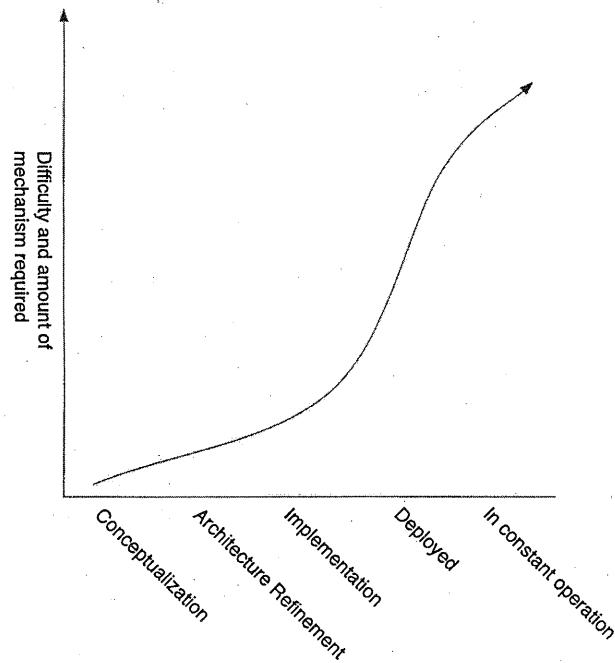


Figure 14-4. Notional relationship between the timing of the identification of a change and the difficulty of and mechanism required for supporting that change

In this figure the steep rise in cost is associated with accommodating change once a system is deployed; the costs top out when a deployed system must be changed on the fly. Deployment adds the costs of dealing with each individual installation of a system – possibly behind firewalls and customized at time of installation. On the fly adaptation requires special mechanisms and circumstances to be achieved, a topic we treat on its own in Section 14.3.3.

Accommodating change early in a project's life is not the same as "fixing problems in the requirements" however. To the extent that types of changes can be identified early in a system's design enables the insertion of mechanisms specifically intended to assist change that happens later. Far beyond a banal "design interfaces to be resilient in the face of potential, identifiable changes to the internals of a module", numerous sophisticated techniques designed to enable broad adaptation have been created. These include plug-in architectures, scripting languages, and event interfaces. These and others will be described in Section 0.

### Change Agents: Their Identity and Location

The processes that carry out adaptation may be performed by human or automated agents, or a combination thereof. Some tradeoffs between these two types of agents are obvious, such as noting that humans can deal with a much wider range of problems and types of change, or that automated agents can act with greater speed. Other issues may not be so obvious. One particular value of automated change agents is in the domain of deployed and continuously operating systems. If an adaptation change agent is part of a deployed application from the outset, the potential is present for an effective adaptation process: getting to the deployed application is not a question. Moreover the agent may have access to contextual information, whereby details of any local modifications and customizations are available. This potentially enables the change agent to act differently in every individual deployment. Users of modern desktop operating systems are familiar with such agents: periodically a user is notified when an OS or application upgrade is available. If the agent is at all sophisticated, the advice given regarding the updates to be performed will be based upon knowledge of any local optimizations. (Often the downloaded update will perform a repeat or supplementary analysis, presenting messages such as "Locating installed components").

In the case of dynamic adaptation the local presence of an automated change agent is essential. Managing the state of the application during the update can be a complicated matter, and is specifically discussed later in this chapter.

### Knowledge

The knowledge possessed – or not – by the change agent can be a major determinant of the adaptation strategy followed. For example, there may be uncertainty surrounding the new behavior or concerning the new properties that are believed to be required. In such a case an adaptation approach that deliberately works to mitigate risk is needed. This might involve processes that allow the engineer to easily retreat from a change in case the change is not satisfactory. Prototyping or story-boarding of potential changes are other strategies that could be employed when there is uncertainty.

Another key aspect of knowledge that governs adaptation strategy is knowing the constraints that must be retained in the modified system. More specifically, an adaptation should be performed with full knowledge of the architectural style of the application. Since the style is (typically) an intangible attribute of a system's structural architecture, knowing it and ensuring that any changes made are consistent with it requires extra work on the part of the adaptation team. The penalty for failing to know and respect the style is architectural degradation. That penalty may not have immediate repercussions, but through the course of successive changes the system's qualities will degrade and the difficulty of performing new changes will increase, sometimes reaching the point where further changes cannot be made at all.

Other important aspects of system knowledge include some obvious things. If the system's architecture has not been retained, then architectural recovery will be required. If a system component is a purchased binary, for which no information is available concerning its adaptation properties (if any), then large-granularity changes will be needed ("component transplants"). If no analysis tools are available to help assess properties of a proposed change, then perhaps a more iterative approach to the adaptation should be followed. When it comes to adaptation, the more knowledge of the system and the change, the better.

### Degree of Freedom

The final aspect of the context of change is the degree of freedom that the engineer has in designing the changes. One might think that greater freedom is always better. Unfortunately greater freedom comes at a significant cost: the search space for solutions is larger, there is less immediate guidance for the engineer on how to proceed, and the assessing all the consequences and properties of a possible change will take more effort. The assumption of this statement, of course, is that the engineer is attempting to do a high-quality job; the cost can always be kept down in the short term by simply adopting whatever adaptation scheme first comes to mind, and doing the work in the same manner or style as the engineer

always does. The price is paid in the future, when, for example, it is discovered that the change inhibits further growth or otherwise degrades the system's architectural quality. The alternate approach is to know or learn the constraints of the application and work within those constraints to satisfy the needs. With this approach coherency is retained and the engineer's energies are directed towards solutions within the current architectural style.

### 14.1.5 Architecture: the Central Abstraction

The final concept of architecture-centric adaptation is the central one: the architectural model. An explicit architecture is latent in much of the preceding discussion. In the absence of an explicit architecture the engineer is left to reason about adaptation from memory and from source code – neither of which has proven very effective in managing change. The presence of an explicit architecture provides a sufficient basis for the planning and execution of system adaptation. Since the architecture *is* the set of principal design decisions governing the system, adaptation based on the architecture proceeds from knowledge of those things which are most intrinsic to the system's design.

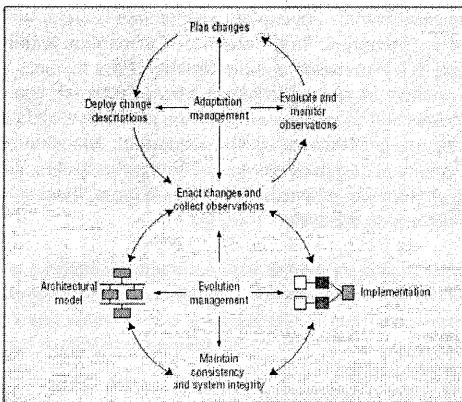
The critical need, of course, is to maintain the integrity of the architecture, and its explicit representation, throughout the whole course of adaptation. As discussed earlier, in Chapters 2 and 9, the most important and most difficult aspect of this task is maintaining consistency between the architecture and the implementation. As long as the implementation is faithful to the architecture, the architecture can serve as the primary focus of reasoning about potential adaptations. As soon as the architectural model fails to be a reliable guide to the code it loses its value for guiding changes; the engineer is left with just the code – the "software engineering" of the 1970's.

Note that apropos of the discussion above about the location of change agents, if the agent is an automated part of a deployed system, then for architecture to be the central abstraction in governing adaptation, the architectural model must either be deployed with the application or communication with an outside reference must be possible. If the model is not available then the agent does not have any basis for architecture-based adaptation unless.

The next section places all the concepts discussed above into a comprehensive framework for architecture-based adaptation.

## 14.2 A Conceptual Framework for Architectural Adaptation

The first comprehensive conceptual framework for architecture-based adaptation was presented in 1999, in [216]. The framework, shown in Figure 14-5, shows the principal activities and entities and key relationships between them. The diagram is simple enough to explain how a very static, requirements-based adaptation process proceeds, but sophisticated enough to indicate how a highly dynamic, automated adaptation process can work.



**Figure 14-5.**  
Conceptual  
Architecture for  
Adaptation. From [216]

Figure 2. High-level processes in a comprehensive, general-purpose approach to self-adaptive software systems.

Quoting from the article,

The upper half of the diagram, labeled “adaptation management,” describes the lifecycle of adaptive software systems. The lifecycle can have humans in the loop or be fully autonomous. “Evaluate and monitor observations” refers to all forms of evaluating and observing an application’s execution, including, at a minimum, performance monitoring, safety inspections, and constraint verification. “Plan changes” refers to the task of accepting the evaluations, defining an appropriate adaptation, and constructing a blueprint for executing that adaptation. “Deploy change descriptions” is the coordinated conveyance of change descriptions, components, and possibly new observers or evaluators to the implementation platform in the field. Conversely, deployment might also extract data, and possibly components,

from the running application and convey them to some other point for analysis and optimization.

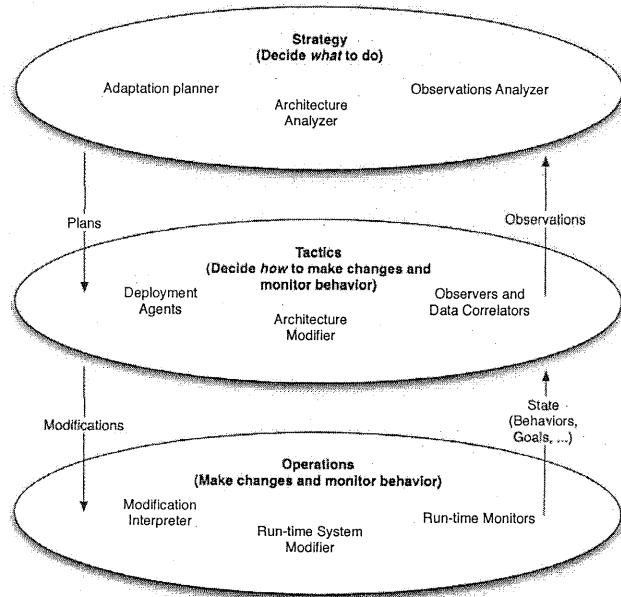
Adaptation management and consistency maintenance play key roles in our approach. Although mechanisms for runtime software change are available in operating systems (for example, dynamic-link libraries in Unix and Microsoft Windows), component object models, and programming languages, these facilities all share a major shortcoming: they do not ensure the consistency, correctness, or other desired properties of runtime change. Change management is a critical aspect of runtime-system evolution that identifies what must be changed; provides the context for reasoning about, specifying, and implementing change; and controls change to preserve system integrity. Without change management, the risks engendered by runtime modifications might outweigh those associated with shutting down and restarting a system.

The lower half of [the diagram], labeled “evolution management,” focuses on the mechanisms employed to change the application software. Our approach is architecture-based: changes are formulated in, and reasoned over, an explicit architectural model residing on the implementation platform. Changes to the architectural model are reflected in modifications to the application’s implementation, while ensuring that the model and the implementation are consistent with one another. Monitoring and evaluation services observe the application and its operating environment and feed information back to the diagram’s upper half.

Figure 14-6 presents a further refined framework. Rather than the somewhat arbitrarily labeled “adaptation management” and “evolution management” of Figure 14-5, this figure separates the activities into three types and shows the entities and agents involved in carrying out the activities. The essential insights of the earlier framework are present, but now with additional detail and precision.

The three activities are characterized as strategic, tactical, and operational. Strategy refers to determining what to do, tactics to developing detailed plans for achieving the strategic goals, and operations to the nuts-and-bolts of carrying out the detailed plans.

Figure 14-6. Activities, Agents, and Entities in Architecture-based Adaptation.



Within the “strategy” activity layer are agents for analyzing information about the system and about the architecture, then planning adaptations based on that analysis. These agents may simply be tasks that a human user performs, or may be automated programs that carry out such tasks.

Within the “tactics” activity layer are agents for making specific architectural modifications based upon the plans received from the strategy layer and deployment agents for seeing that those modifications are conveyed to all deployed instances of the architecture to be modified. Also found here are agents for determining how to correlate raw monitoring information received from deployed instances of the system such that the collected data is suitable for analysis at the strategy level.

Within the “operations” activity layer are the specific mechanisms for modifying the architecture models (such as may reside on deployed instances) and modifying the implementation, maintaining consistency between them, and mechanisms for gathering data from an executing instance.

Keep in mind that one purpose of a framework such as this is to provide the engineer with a checklist of issues. Not all parts of the framework will be equally useful in all adaptation contexts. Similarly the location of the various entities involved (both the agents performing the changes and the entities being analyzed or being changed) may vary. The architectural model is a good example: any agent that needs to analyze or modify the architecture must have access to it. If the application is embedded an isolated, autonomous system, then all the agents required, and the model, must be present on that system. If on the other hand the system can be stopped, reloaded, and restarted, all the adaptation agents and models may be found (only) on the development engineer’s workstation. The deployment activity might only involve the object code.

## 14.3 Techniques for Supporting Architecture-centric Change

In this section we first present a selection of techniques which can be used to support the activities of the conceptual framework presented above, such as observing the application state and modifying the architecture. Since not all architectures or architectural styles are equally adept at supporting adaptation, we then present an overview of styles – some more architectural than others – which facilitate change. The section concludes with discussion of the special problems of autonomous change.

### 14.3.1 Basic Techniques Corresponding to Activities of the Conceptual Framework

Adaptation is triggered when someone – user, developer, auditor – determines that the current behavior of a system is not what is desired. That determination is based upon observation, the cornerstone activity.

#### Techniques for Observing and Collecting State

Determining what techniques are most useful for observing and collecting state information presupposes knowing what “state” is. In its most obvious form “state” consists of the run-time values of a program’s objects. Since values are continually changing, state is relative to time, and since only a small subset of a program’s state is likely to be of use in adaptation, the observed state is usefully a time-stamped sequence of a subset of the run-time values of the program’s objects.

Other information beyond values of a program’s variables may also be important parts of “state” used for adaptation purposes. For instance, properties of the program’s environment that are not represented in the program may be essential in determining how an application should be adapted. It may be, for example, that the behavior of a system should be a function of some currently unrepresented attribute of the external environment. An automated teller machine, for instance, should perhaps enter a safe mode and wirelessly signal an alarm whenever the ATM is

subjected to G-forces in any direction (such as might be caused by an earthquake – or by someone attempting to abscond with the machine). Gathering this enhanced notion of a program's state would entail monitoring more than just the program.

A more prosaic example of external information that may be critical in determining an adaptation strategy is deployment information. The behavior of a system may be impacted by the presence of certain platform specific options – the presence of certain device drivers, the amount of memory available, or the version of the operating system, for instance. Such information is usually easy to gather (e.g. from “registries” such as MS Windows registry database or Mac OS X’s library files) and may be essential in the analysis phase.

System specifications and the system’s architectural model may also be aspects of state that need to be observed on the target system and brought to the analysis context. One might expect this information to be static and already known to the adaptation analyst/planner, but in some contexts that may not be true. For example, if an application is highly configurable, each running “instance” of the application may be unique – perhaps because of customization to reflect installed hardware options. This information is thus akin to the deployment information mentioned above: in that case the “site-specific information” concerns properties external to the application to be adapted; in this case the information is about the application itself. The observed architecture, therefore, is the architecture of the application as it exists in its fielded state. Its set of components, connectors, and their current configuration may be unique. In some more esoteric situations, such as autonomous adaptation, the fielded system may also contain explicit and dynamically changing goal specifications for the application. These would also constitute part of the state subject to observation and reporting to the adaptation analyst.

#### *Gathering the State*

Numerous techniques exist for gathering the state of a program’s objects; the numerous techniques developed to support program debugging all apply. Most primitively, the analyst may manually observe the program’s user interface. More usefully, observation code may be part of a special run-time system that enables monitoring of a program without requiring any modification to it. In some contexts, such as specialized embedded systems, “bolt-on” hardware analyzers may allow inspection of program state without any disturbance to the run-time software environment.

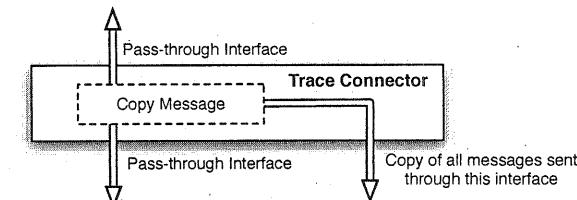
If modification of the subject software system is feasible, a variety of more specialized and targeted approaches are possible. Again, at the most primitive level, the beginning programmer’s technique of seeding a program with print statements may be sufficient. As program and problem

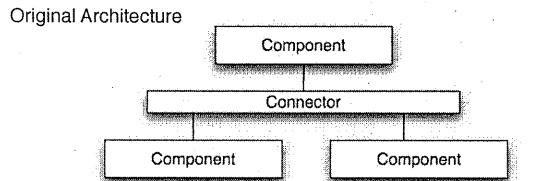
complexity increase more powerful and thoughtful approaches are required. Customized monitors may be inserted in the application code, and function similarly to assertions. Such assertions can check for specified conditions, and if satisfied record some value or otherwise emit an “observation” of the program’s state. Whether a given programming language’s assert statement is appropriate for this use depends on the language semantics: if satisfaction of the assert necessarily interrupts the program’s flow of control following the assertion, then use of that language feature would not be appropriate. Monitoring should allow execution to proceed unimpeded.

To the extent that creation of custom monitors is a manual process, it is an expensive process. Moreover the use of custom monitors such as described above is only feasible when the source code is available and the application can be recompiled. One alternative is to focus on capturing information only at component boundaries, and to do so by capturing information that passes through an application’s connectors. This technique can be based upon commercial middleware when used for connectors, or may take other forms. If the information gathering is automatic and does not filter “uninteresting” data, then it must be coupled with other tools to support filtering after the raw data has been gathered.

The concept is illustrated by the MTAT system [118], which creates a log of all messages sent between components in an architecture during its execution. This log is created by automatically instrumenting an architecture with trace connectors (see Figure 14-7). Trace connectors intercept all messages passing through them, make a copy of each message, and send the copy to a distinguished component that logs each message in a relational database. The original messages are passed on unmodified. The trace connectors are first-class connectors, and are not part of any component in the architecture. Figure 14-8 shows an architecture before modification as well as the architecture after inserting trace connectors.

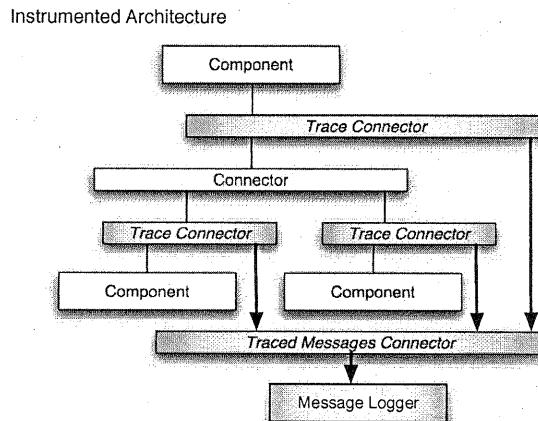
Figure 14-7. A Trace Connector





**Figure 14-8.**  
Instrumented  
Architecture and  
Original Architecture.

Above is the architecture to be traced. Below is the architecture as it is actually instantiated. Trace Connectors echo every message received on their top or bottom interface to the Traced Messages Connector, which forwards each message to the Message Logger.



The MTAT analysis system includes a tool that examines a xADL description of a system's structure and inserts trace connectors into that description automatically. The system's structure is modified so that each link in the original architecture is split into two links, with a trace connector between. Because the infrastructure provided by xADL and its supporting ArchStudio tool set instantiates architectures directly from their descriptions, no recoding of components is needed for instrumentation. Consequently, components in the application remain unaware of any architectural changes or the presence of the trace-connectors once the architecture is modified. The approach works in both single-process and distributed systems. In distributed systems, connectors that bridge process boundaries are broken into two halves—one in each process they connect. In terms of instrumentation, distributed connectors are treated the same

way single-process connectors are; a trace connector is placed on every link in every process.

Finally, depending on the adaptation context, the technique used for gathering the observations may also need to be responsible for transmitting them from the platform where the target application is running to the host where the adaptation analysis will take place. To the extent that the target is an embedded system this off-board transmission is likely to be a necessity.

### Techniques for Analyzing the Data and Planning a Change

#### Analyzing the Data

Analyzing the data gathered from observing a system and consequently determining what adaptations to perform is wide open problem. The range of types of changes that may be required precludes the prescription of a small set of standard techniques. Indeed, the problem is essentially the same as program understanding and program debugging. For some situations a simple, canonical technique may suffice. For most situations ample human thought will be required.

To the extent that kinds of change may be anticipated while a system is being designed, techniques may be put into place to monitor for specific situations, triggering pre-planned strategies for coping with the change when the monitors detect the key values. The data "analysis" is simply comparing a value to a reference. Consider the example of an electronic commerce application. As the number of customer transactions increases the back-end servers must perform more work. As a maximum threshold is approached additional servers must be brought on line to avoid degradation of the user experience. Since much of the transaction processing in such e-commerce applications can be performed by independent servers, a simple load-sharing design can be used wherein additional servers are brought on-line automatically, becoming part of the "server farm," as the result of monitoring a threshold value and triggering the pre-planned response.

An easy step up from this situation is using a set of rules to monitor a set of observed values. The guarding conditions in the rules may be complex; so too may be the corresponding actions. In essence, though, the approach is the same: the system's design has explicit provision for accommodating anticipated change, including the specific approach for monitoring and analysis. One use of this technique might be in comparing observed behavior of a system with behavior predicted by an analysis of the architecture before its implementation. For example, a simulation may show that a system correctly aborts a transaction if any one of its sub-transactions fails; but monitoring of the implementation may show that the transaction was (inappropriately) completed in such a case.

Beyond these simple approaches there are few general techniques focused on analyzing observational data to guide adaptation. One example is illustrative, however. The MTAT system mentioned above is targeted at helping engineers understand the behavior of applications having an event-based architecture. The trace connectors shown in Figure 14-7 feed copies of all messages sent in the architecture to a relational database. This database can then be examined in various ways to determine, for instance, communication patterns in the application or causality chains. Causality chains are particularly useful: when an engineer understands that message  $a$  from component  $A$  causes message  $b$  to be sent from component  $B$  and so on, changes can be made that reflect a deep understanding of the interrelationships between elements of a system's architecture. Note that in essence this approach is similar to techniques employed in debugging source code; the difference is in bringing the analytic approach to bear at the level of architectural concepts, and focusing on the particular kind of communication used at the architectural level.

#### *Analyzing the Architecture and Proposing a Change*

Assuming that observations of a system have been obtained and analyzed, it remains to develop a modification to the architecture to meet whatever needs the architect is concerned with. Again, the challenge may be very simple or very complex.

If the architecture was originally designed to accommodate certain types of change, and analysis of the data shows that the needed change is within the expected scope, then proposing a responsive change is straightforward. For instance, if a component is shown to be a performance bottleneck, and a faster replacement component having the same interfaces can be produced (i.e. the change is confined to the component's internal "secrets"), then simply swapping the original component for the improved one is all that is required. If a system's architecture is in the client-server style and a new client is needed, modification is simple. If a system's architecture is in the publish-subscribe style and a new publisher is available, then again the path to change is straightforward. The pattern here is clear: if the change needed fits within the type of change anticipated and accommodated by the application's architectural style, then the approach to take is clear.

If analysis shows that the needed change does not fall within an anticipated pattern, then the architect has to revert to the general analysis and design techniques discussed earlier in Chapters 4 and 8.

#### Patches, Service Packs, Upgrades and Releases

Commercial systems use a variety of techniques and terminology in supporting "upgrades" of deployed software products. The terms "upgrades", "releases", "service packs", "patches", and others are all used. There is little consistent technical meaning for these terms. Patches were initially used to refer to small changes to a file, but some have used the term for what amounts to wholesale replacement of the original file. Patches can be applied to binary files as well as textual. The term service pack is usually used to denote a collection of changes to an application, but there is no consistency on this either.

The means of deployment and installation of patches (whichever term is used) can vary significantly. Some deployments are initiated by the deployed software itself – that is, an instance of a system checks with the "home site" for available upgrades, and if found proceeds to initiate a download. In other occasions the vendor will initiate the deployment, attempting to notify all user sites of the need for the upgrade. Once deployed the patch may be installed automatically or may require active user involvement.

The installation activity may be unsophisticated, or may involve checking the context – what other components or applications are installed which might determine the particular change to make.

All these activities echo or embody some of the techniques involved in a robust architecture-based adaptation process, such as described in this chapter.

#### *Analyzing the Proposed Change*

After a proposed change to an architecture has been developed it should be checked to determine if it is complete and appropriate for deployment to its target platforms. Checking a proposed change seems so obvious that it should go without saying, but consider some of the possible items that may need to be checked:

- Are there any unattached ("broken") links in the new architecture?
- Have all interface links been type-checked for consistency?
- Are all components properly licensed for use in the target environments? (E.g. if the target environment is a commercial product, do any of the new components have GPL licenses attached?)
- Are communications between the components performed consistently with the application's security requirements? (E.g. if two components communicate over an open network, are the messages encrypted?)

- Is every component and connector in the revised architecture mapped to an implementation?
- Is everything in the deployment package that the change agent on the target platform requires? (E.g. license keys and configuration parameters.)

The number of issues that may need to be checked is large, and hence an explicit process step to verify them is usually warranted.

One situation that calls for special attention is when each target system to which the revised architecture is to be deployed may be unique. That is, due to the possibility of local modifications, each target needs, in essence, to be individually checked. If the number of targets is at all significant the analysis will have to be automated.

#### **Techniques for Deploying Change Descriptions and Modifying the Architecture**

##### *Describing changes to an architecture*

To effect a repair on a running software system, the changes to the system that will occur because of the repair must be specified and machine-readable. There are three primary ways that concrete architectural changes can be expressed. These are:

- **As “change scripts:”** Change scripts are executable programs that operate on a system to make changes. In general, these scripts leverage underlying adaptation APIs provided by the implemented system (or its architecture implementation framework or its middleware). Adaptation APIs provide high level functions for, e.g., instantiating and removing components and connectors, creating and destroying links, exposing or withdrawing provided services, and so on. Sometimes, change scripts will be accompanied by implementation artifacts (e.g., new source or binary files) that are merged with the implemented system.
- **As “architectural differences:”** Rather than executable programs or scripts, architectural changes can be expressed as a set of differences between one architecture and another. In general, these differences, also known as “diffs,” contain a list of additions, removals, and (optionally) modifications to architectural elements. For example, a diff might indicate the addition of two components, new interfaces on those components and others already present, and new architectural links to hook those components into the architecture, as well as the removal of links that are no longer needed. Given two concrete architectural models of the system as it is and the system as it should be, tools can create a diff automatically.

- **As completely new architectural model:** In some cases, especially cases where the current state of the system to be adapted is unknown, a complete architectural model is used to describe the target adaptation architecture. In this case, an architectural difference is generally created by examining the elements in the current system as well as those in the new model and determining what to add and remove to bring the current system in line with the new architecture. Whether or not this architectural difference is expressed as a new artifact or is simply a side effect of determining the changes depends on the approach.

##### *Applying Changes to an Architecture*

In any of these three cases, two worlds are involved—the world of architecture and the world of implementation. In general, for any of these change artifacts to be effective in adapting a real, implemented system there must be a tight correspondence between elements in the architectural model and elements in the implementation. The use of architecture implementation frameworks or flexible middleware (see Chapter 9) can be used to achieve this. Otherwise, the architectural changes are simply changes to the system’s design, and cannot be automatically applied to a real software system.

In the absence of tight bindings between architecture and implementation, it is conceivable to employ a human as the change agent on the target system. That is, the change artifact is reviewed by a person, and that person is responsible for making the corresponding changes to their system. This is an unorthodox strategy since end users are rarely asked to redesign the software systems they are running, and as far as we are aware it is rarely (if ever) used in practice. One exception to this might occur in the case of software systems with complex deployments. Certain software systems (for example, enterprise resource planning (ERP) systems) are so complex to deploy, install, and configure that customers simply cannot do it themselves. In general, an organization that purchases the software also hires a team of consultants or product experts to deploy, install, and configure the software for their own organization. In this case, architectural changes might be deployed from the vendor to the consulting team, who can then make the configuration changes to the system manually.

Once changes to a system’s architecture are described concretely in one of the above forms, they must be actually applied to that system at run-time. In the case of change scripts, the change script is executed in some run-time environment co-located with the target application. Software underlying the target application, usually the architecture implementation framework or middleware, is called upon to actually make the changes to the system. In the case of architectural diffs, a change agent running alongside the target application must interpret the diff and make the

changes specified therein, a process known as merging. In the case of new architecture specifications, a change agent must determine the difference between the current and intended application configuration and make changes as needed.

#### *Issues with Deployment*

No matter what form of change artifact is used—change scripts, architectural diffs, or new architectural specifications—that artifact needs to be deployed to the target system (or its associated change agent). The issues involved with deploying these change artifacts are similar to those found in software deployment in general, and so most of the advice in Chapter 10 on deployment applies here as well. If the target system is running on a single (remote) host, deployment is generally straightforward: the change artifact can be sent over any number of network protocols such as HTTP or FTP to the change agent, which then executes the changes. Distributed and decentralized systems can use push-based or pull-based approaches to distribute change artifacts.

In any of these approaches, a change agent must be located on the target machine to actually effect the changes on the architecture—to execute the change script, to parse the architectural diff, and so on. This agent can be deployed with the original system, or it can be sent along with the change artifact. For example, a change script could be compiled into executable form (as an ‘installer’ or ‘patcher’) and then sent over the network to the target system, where it is executed by the operating system directly. This is convenient as it avoids the problem of having to update change agents themselves. This strategy carries some security risk—running arbitrary executables on target platforms is an easy way to spread malicious software if the code is not trusted. Code signing and other strategies can be used to mitigate this risk.

#### *Issues with Applying Changes*

Making on-the-fly architectural changes (see Section 14.3.3 below) is more difficult. All issues identified below with respect to ensuring that the application is in an appropriate ‘quiescent’ state to be adapted apply with these strategies. Making on-the-fly changes to a distributed system is even more difficult, since the change must first be deployed to all appropriate parts of a distributed system, and then the system as a whole must be put into a quiescent state for update. This involves additional risk, since network and host failures during the update process can make it difficult to get the system into a consistent state.

#### **An Example Comprehensive Instantiation: ArchStudio**

The ArchStudio environment supports architecture-based adaptation with a combination of techniques listed above. Specifically, it uses an architecture implementation framework to ensure a mapping between architecture and implementation. Then, architectural diffs are used as

change descriptions to evolve a system at run-time. The process for evolving a system occurs in four steps.

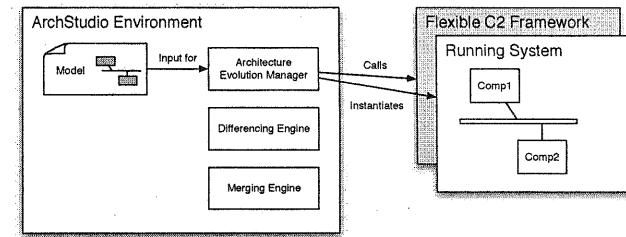


Figure 14-9.  
ArchStudio adaptation  
step 1: instantiation.

Step 1 of the process is shown in Figure 14-9. An architecture description in xADL is provided to a tool in ArchStudio, the Architecture Evolution Manager (AEM). The AEM reads through the model and uses the Flexible C2 Framework, described in Chapter 9, to instantiate the system. Implementation bindings in the xADL model facilitate the mapping from architectural components and connectors to Java components.

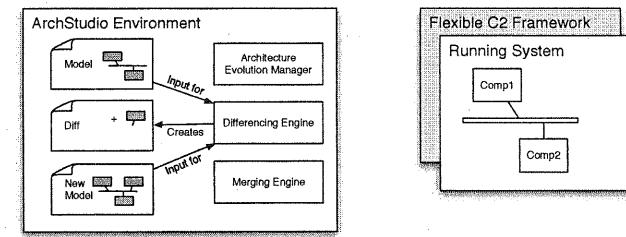
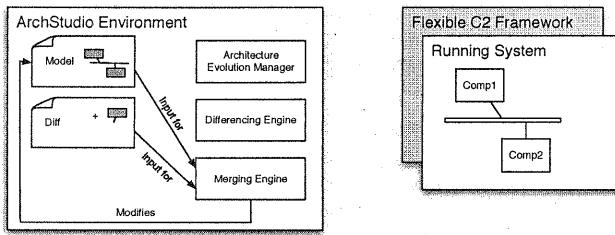


Figure 14-10.  
ArchStudio adaptation  
step 2: differencing.

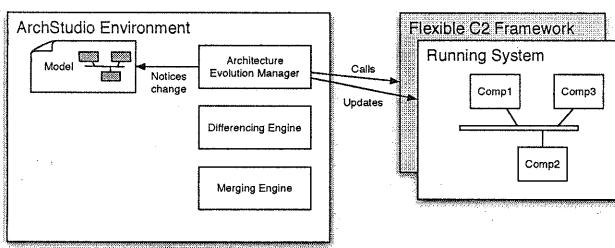
Step 2 of the process is shown in Figure 14-10. A new architectural model is created in the environment, possibly by making a copy of and modifying the old model. Then, the old model and the new model are both provided as input to another ArchStudio tool, the differencing engine ‘ArchDiff.’ ArchDiff creates a third document, an architectural diff, that describes the differences between the two.

**Figure 14-11.**  
ArchStudio adaptation  
step 3: merging.



Step 3 in the process is shown in Figure 14-11. Here, the new model is no longer needed. The original model, still describing the running system, and the diff are both provided as input to another ArchStudio tool, the merging engine ‘ArchMerge.’ The merging engine, acting as a change agent, modifies the original model with the changes in the diff.

**Figure 14-12.**  
ArchStudio adaptation  
step 4: applying  
changes.



Step 4 in the process is shown in Figure 14-12. Here, the AEM notices that changes were made to the original model (by way of events emitted from the model repository within ArchStudio). AEM then makes the corresponding changes to the running architecture by making more calls to the underlying Flexible C2 framework, instantiating new elements and changing the application as necessary. Although only additions are shown in these simple diagrams, ArchStudio supports additions, modifications, and removals of elements.

#### 14.3.2 Architectures/Styles that Support Adaptation

The preceding sections focused on generic techniques that support parts of the conceptual framework for architecture-based adaptation which was presented in Figure 14-6. The difficulty of making changes – even using these techniques – will vary enormously from one application to another,

however, depending on the type of change required and the nature of the architecture to be changed. The discussion of shearing layers early in this chapter indicated, in generic terms, why some changes are more difficult to effect than others. The discussion of the many architectural styles in Chapter 4 showed in particular how some styles are more adept at handling particular types of change than others. Client-server architectures, for example, are designed to easily accommodate the addition or deletion of clients.

In the subsections below we revisit the topic of styles, introducing some specific interface-focused architectural approaches to facilitating change, and then briefly reconsider some concepts from Chapter 4 which are particularly effective in supporting change.

#### Interface-focused Architectural Solutions

Since developers have been tasked with changing software since the advent of computing it is no surprise that a variety of techniques have emerged to help this process. The techniques presented here all reflect application of the dictum “design for change”. We have categorized these techniques as interface-focused since they rest upon application-programming interfaces or interpreter interfaces presented by the original application.

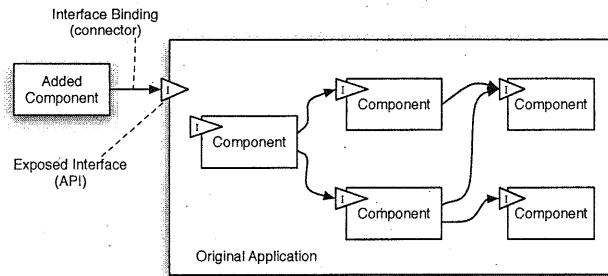
These techniques do not purport to support all types of change. Indeed, the primary focus of these techniques is only in *adding* functionality in the form of a new module.

#### Application programming interfaces (APIs)

APIs are perhaps the most common technique for enabling developers to adapt an application by extending it. With this technique, the application exposes an interface—a set of functions, types, and variables—to developers. The developers may create and bind in new modules that use these interface elements in whatever way the developers choose. (The interrelationships between the new modules themselves are unconstrained by the API.) The type of change to the original application that can be supported is limited to whatever functionality the API presents. Many operating systems and commercial packages use APIs.

This approach is illustrated in Figure 14-13, which presents a notional picture of an application to which one new component has been added. The added component can make use of any of the features of the original application that are exposed by the API, but it cannot access the interfaces of any of the components internal to the application, nor can it modify any of the connections internal to the application. The added component makes calls to the original application; nothing in the original application can make calls to the added component.

Figure 14-13. Using an API to extend an application with a new module.

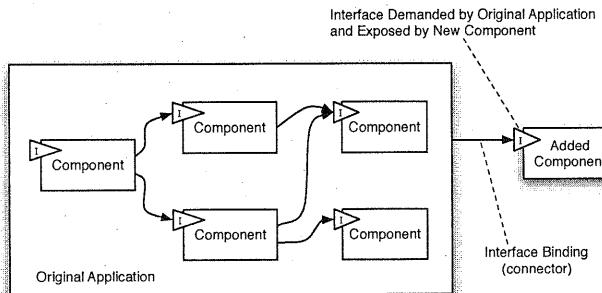


#### Plug-ins

Plug-ins are sort of a mirror-image of APIs: instead of the added component calling the original application, the application calls out to the added component. To achieve this the original application predefines an interface that third-party add-ons or “plug-ins” must implement. The application uses and invokes the plug-in’s interface, thereby altering its own behavior. To initiate the process the original application must be made aware of the existence of the plug-ins; they must become registered with the application. Typically the registration happens on application start-up, when the application inspects pre-defined file directories. Components found in those directories that meet the interface specification are registered and may then be called.

The technique is illustrated in Figure 14-14.

Figure 14-14. Using a plug-in interface to extend an application.

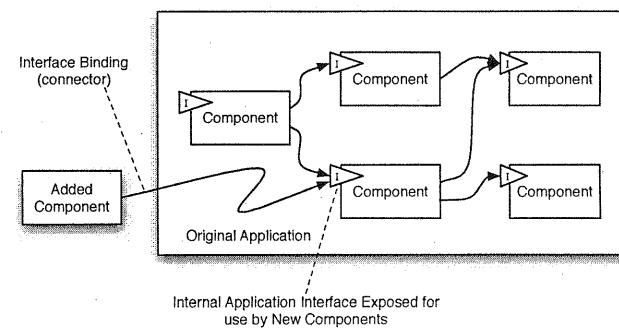


Adobe Acrobat and Adobe Photoshop are applications which historically have made significant use of the plug-in mechanism. Direct interactions between multiple plug-ins are possible, but such interaction is not part of the plug-in architecture.

#### *Component/object architectures*

With this technique, the host application exposes its internal entities and their interfaces to third-party developers so that they can be used during the adaptation process. This is in contrast, for example, with the API and Plug-In approaches which view the original application as a monolithic entity whose internal structure is opaque and immutable. Here, add-ons alter the behavior of the host application by adding new components that interact with existing components. Exposing the internal entities also allows a component to be replaced by one that exposes a compatible interface. This approach is illustrated in Figure 14-15.

Figure 14-15.  
Application modification via the  
component/object architecture approach.



Examples of systems that follow this approach include applications built with Microsoft’s Component Object Model (COM).

This approach to adaptation is more powerful than either APIs or Plug-Ins, since more interfaces are exposed, and the approach seems architecture-centric since the key items in the vocabulary are a system’s components. Typically missing in common application of this technique, however, is an explicit architectural model. The developer is (just) confronted with the system’s source code; nothing at a higher level of granularity that can be manipulated to achieve the desired changes.

CORBA-based systems, discussed in Chapter 4, are members of this category. Such systems can be very fluid, but management of them can

be difficult because there is no explicit model capable of serving as the fundamental abstraction.

#### *Scripting languages*

With this approach the application provides its own programming language (the “scripting language”) and runtime environment which the architect uses to implement add-ons. In essence this is a use of the Interpreter Style from Chapter 4. Add-ons, when executed by the interpreter, alter the behavior of the application. Scripting languages commonly provide domain-specific language constructs and built-in functions that facilitate the implementation of add-ons, especially for users who lack programming expertise. Spreadsheet formula languages, macro systems, and programming-by-demonstration systems are essentially scripting languages optimized for specialized needs. Microsoft Excel is a prime example of an application that provides this means of extension.

The technique is illustrated in Figure 14-16.

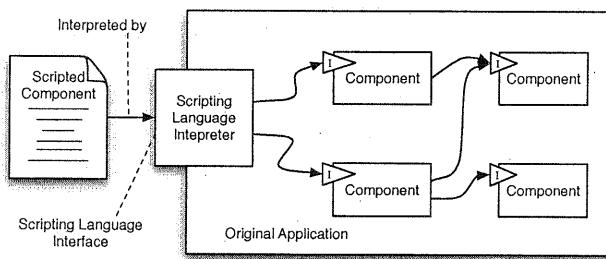


Figure 14-16.  
Application adaptation  
by means of a scripting  
language.

#### *Event interfaces*

With this technique – a simple application of the event-based architectural style of Chapter 4 – the original application exposes two distinct interfaces to third-party developers: an incoming event interface, which specifies the messages it can receive and act on; and an outgoing event interface, which specifies the messages it generates. Messages are exchanged via an event mechanism. Add-ons alter the behavior of the application by sending messages to it or by acting on the messages they receive from it. As discussed in Chapter 5, event mechanisms commonly provide a message broadcast facility, which sends a message to every add-on attached to the event mechanism. The event mechanism acts as an intermediate, encapsulating and localizing program binding and communication decisions. As a result, these decisions can be altered independently of the original application or add-on components. This is in

sharp contrast to the other techniques, in which programs directly reference, bind to, and use each others interfaces. The technique is illustrated in Figure 14-17.

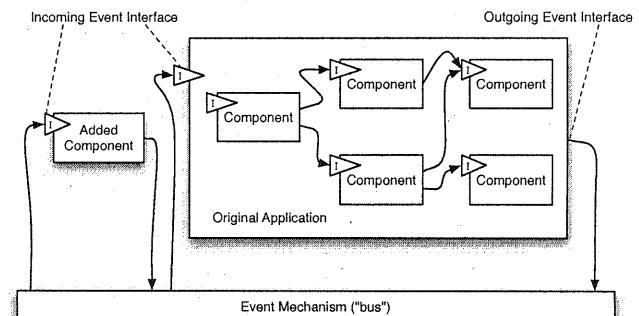


Figure 14-17. An event architecture used to support extension.

#### **(Strong) Architecture-Based Approaches**

Should changes to a system be required that involve more than just adding a new module, a richer approach to adaptation is needed than what the interface-focused solutions above offer. The core of any architecture-based solution, as we have discussed, is an explicit architectural model, faithful to the implementation, which can serve as the basis for reasoning about changes.

Simply having an explicit architecture is no panacea, of course. Complex dependencies between architectural elements and inflexible connectors may render difficult any adaptation problem. Consistent use of any of the architectural styles of Chapter 4 can remove of the inherent difficulties. Ill-conceived custom styles that combine simpler styles in complex ways can vitiate those benefits, however.

The fundamental issue is *bindings*. To the extent that an architectural style enables easy “detachment” and “attachment” of components from one another, that style facilitates adaptation. The consistent emphasis of this text on the use of connectors stems from the benefits that explicit connectors can provide in supporting such attachments and detachments. The wide range of connector techniques discussed in Chapter 5 reveals that not all connectors are equally supportive of adaptation, however. Since a direct procedure call is one kind of connector it is obviously possible for the internals of one component to be strongly tied (via a procedure-call connector) to the details of an interface provided by another component. In the extreme (and hence rather useless) case of treating

shared memory as a “connector”, arbitrary interdependencies between components may be “achieved”. These negative examples do serve to indicate what makes a good connector, and what makes a style supportive of adaptation: independence between components. At a minimum this means lack of dependency on interfaces. (As we shall see later, however, this is not a sufficient condition.) Use of particular types of connectors can achieve this independence, wherein one of the roles of the connector is to facilitate communication between two components while insulating them from dependence.

Perhaps the best example of this kind of connector and the independence provided is event-based connector discussed in Chapter 4 in conjunction with the implicit invocation architectural styles. Components send events to connectors which route them to other components. The events are capsules of information; the sending component may not know what components receive the sent event; a receiving component may not fully understand all the information in the event, but still can process it such that its own objectives are satisfied. A network protocol (such as HTTP/1.1) can be used, for example, to support this type of communication. The protocol supports moving MIME-encapsulated data throughout a distributed application; how a receiving component interprets and processes the encapsulated payload is a decision local to that component. Ensuring that the collection of components and connectors cooperate to achieve the objectives for the application is the responsibility of the system architect. For detailed examples of this type of architecture, see Chapter 4, including the discussion of the C2 style.

#### 14.3.3 The Special Problems of On-the-fly and Autonomous Adaptation

Adapting a system while it remains in operation presents special challenges, complicating the adaptation process. Some example situations where that complication cannot be avoided were given at the beginning of the chapter. These include applications whose continuous operation is essential to the success of some larger system, such as control software in a continuously operating chemical refinery.

Autonomous adaptation means that human involvement in the adaptation process is absent, or at least greatly minimized. Autonomous adaptation can be a complicating addition to on-the-fly adaptation, such as when the continuously operating system is isolated from external control, such as in robotic planetary exploration. Such extreme circumstances are not the only ones where autonomous adaptation may be required, however. It may be, for instance, that rapid response requirements to partial system failure dictates the use of autonomous adaptation techniques.

Some of the challenges of on-the-fly adaptation can be seen through analogies. Living in a house that is undergoing a major renovation is sometimes necessary, and is seldom pleasant. The unpleasantness comes from attempting to carry on daily life while portions of the service architecture that we depend upon – plumbing, electricity, heat, security, and so on – are only partially or intermittently available. Life goes on, but not in the regular rhythms or with the usual comforts.

A more vivid, and instructive, example is surgery. The patient corresponds to the system being “adapted”. Clearly it is essential that while the adaptation is taking place – repair to a heart valve, for example – the patient must be kept alive. The various subsystems of the human (must) continue to function even though major disruptions take place. The various techniques and technologies of heart surgery, from anesthesia to cardiopulmonary bypass, are designed to maintain basic system performance while enabling major restructuring of a key component.

The key additional issues in on-the-fly adaptation are:

- Service strategy: while the adaptation is taking place, will the system continue with a temporary service to fully replace the one being changed? Will it continue with a reduced level of service? A missing service? Can some service errors be tolerated? System functioning during adaptation may be maintained through the use of auxiliary components (such as the heart-lung machine in the surgery analogy), or may be degraded to a lower level of functionality (such as using a bathroom sink to wash dishes while the kitchen is remodeled in the home remodeling analogy).
- Timing: identifying the occasions when the subject parts of the system can be altered. Depending on the service strategy adopted, the conditions under which the adaptation may proceed can be identified. Replacement of a component may only be allowed, for example, when it has finished servicing all outstanding requests to it, and has not initiated any requests on other components in the application.
- Restoration or transfer of state. If a component is replaced, does the replacement component need to know some or all of the state information (“variable values”) that was held by its predecessor? The first calculations made by the new component may necessarily be functions of previous values computed and stored, in which case that state would have to be restored at the time the new component is started up.

An example may help make these concepts more clear. (Throughout this section we assume, consistent with the preceding parts of this chapter, that the smallest unit of change is a component and that component identity and boundaries are maintained in the implementation.)

Consider first the example of a processor that controls the opening and closing of a valve in a chemical refinery based upon command inputs, temperature sensors, and flow meters. It may become necessary to replace one of the control components on board, due to identification of an error in one of its algorithms. Such a processor may be designed in the sense-compute-control pattern discussed in Chapter 4. One plausible adaptation strategy is, at an arbitrary time, to cease processing of any incoming signals on its sensors, leave the valve's opening at whatever position it is in, swap out the offending component, swap in the new component, and then start the replaced component by first sampling all the input sensors, and thence issuing new commands to the valve. Whether this strategy will work depends on, for example, whether any inputs missed during the swap were critical to the refinery's safety, or whether leaving the valve open in its last position could endanger the refinery before the new component was in place. For instance, if the valve was left in the "full on position" while the upgrade was taking place, and if the upgrade took very long to transpire, some downstream reaction in the refinery may be put at risk. A better strategy would likely entail buffering all inputs to the valve controller so that when the new component comes on line it would ensure that every incoming value was processed, and instead of leaving the valve at its "last level," putting it into some "safe state".

The appropriate service strategy for this example would likely be determined in consultation with the plant's chemical engineers. The amount of time the control processor could safely be pre-occupied with the adaptation might well be determined by properties of the chemical processes in the refinery. If the valve is highly critical a temporary controller may need to be put into place. Timing of the adaptation could be determined by properties of the plant, or perhaps by the state of the valve itself (perhaps the adaptation would occur only when the valve is closed).

#### Determining the Conditions for When to Effect a Change

The determination of the precise conditions under which it is appropriate to replace a component can be a function of the application as well as of the architecture. The application, as illustrated in the refinery example, may dictate that change happen only under certain external conditions. Alternatively, application domain analysis may reveal that change can happen at any time – even if it means that some outputs produced are erroneous – simply because the application is so robust that it can tolerate some significant degree of error on the part of the computer system. For example, a satellite that gathers weather data, processes it, and sends the resulting information to the ground may be in this category. Weather data is continuous and is a phenomenon which changes slowly (relative to computer processing, at least), so simply losing some amount of the telemetry data is unlikely to matter.

Some applications will demand a much more conservative analysis, however. The principle is that it is safe to remove/replace a component only when such change will not adversely affect the functioning of the rest of the application. While precisely identifying all such conditions may be quite difficult, it is easier to specify sufficient conditions. Some sufficiency conditions are captured in the notion of *quiescence*. The intuition is that it is safe to replace a component when that component is inactive. A simple understanding of quiescence is that the component is not engaged in sending or receiving information, and internally is idle (all of its threads are idle). Inactivity, however, needs to be understood more comprehensively, in terms of any transactions to which the component may be a party. That is, a component  $C$  may initiate a set of actions that are performed by other components, itself staying inactive until the other components complete their task and return control to  $C$ . In this case  $C$  is not quiescent until all actions that are part of a (conceptual) transaction are complete. Various shades of quiescence are defined in the sidebar, drawing from the work of Kramer and Magee, who pioneered this area.

If an application is implemented with powerful, explicit connectors, such as message buses, then determining whether a component is engaged in communication is easy – the connectors may be used to make this determination. Knowing whether a component is engaged in a multi-party transaction, however, requires deeper analysis and will have to consider the behavioral characteristics of the architecture as a whole. The stronger the notion of quiescence required the more complex will be the determination of when it is achieved.

Quiescence, according to Kramer and Magee:

A node in the active state can initiate and respond to transactions. The state identified as necessary for reconfiguration is the passive state, in which a node must respond to transactions, but it is not currently engaged in a transaction that it initiated, and it will not initiate new transactions. This passive state is so defined as to permit connected nodes to progress towards a passive state by completing outstanding transactions. In addition it contributes to system consistency by completing transactions. For consistency during change we require a stronger property, that the node is not within a transaction and will neither receive nor initiate any new transactions i.e. all outstanding transactions are complete and no new ones will be initiated. Change quiescence of a node is defined as that state when the node is both passive and there are no outstanding transactions to which it need respond. Such a state depends not only on the node itself, but on the connected nodes.

-- from "Change Management of Distributed Systems" [154].

### Management of State

A component's *state* is the set of values that it maintains internally. When a component *A* is replaced with a component *B*, the question arises as to what *B*'s state should be initialized to upon its startup. The easiest situation is one where no transfer or recreation of corresponding state is needed. For example, many Unix filters do not maintain state; the output they produce is solely a function of the most recently read input, unaffected by any preceding computation. Other applications may not be so designed; for instance the user may have set a number of preferences; should the application be modified while the user is working with it, the preferences should be transferred. One effective strategy for dealing with transference of state is simply to externalize it: copy whatever state needs to be moved to a "third party"; when the replacement component comes on line its first action is to initialize itself by drawing from the third party. This strategy, of course, presumes that the components were designed for replacement – a condition not often true.

### Practical Tips

While the principles and issues discussed above apply to architectures generally, there are some practices and approaches which definitely ease the practical problems of supporting on-the-fly adaptation. Foremost are use of explicit, discrete, first-class connectors in the implementation and use of stateless components. To see the success of this simple advice, consider the architecture of the Web. As described elsewhere in this text the Web is based upon these principles – and manifestly the Web is an application which is continuously undergoing change. Proxies and caches can be added and deleted; new web server technologies put into place, new browsers installed. It all works because the interactions between the various components are discrete messages and the core protocol (HTTP/1.1) requires interactions to be context-free ("stateless" in the Web jargon) – a server does not need to maintain a history of interactions with a client in order to know how to respond to a new request.

### Autonomous Change

Autonomous change is adaptation undertaken without outside control. The distinctive character of autonomous change is not the challenge of working without connection to, say, the Internet, but rather effecting the change process without involving humans. The desire to avoid involving humans is readily motivated: a self-adaptive system can change much more quickly than one involving people; consequently self-adaptive change is likely to be much cheaper. Other situations may similarly motivate autonomous change. For instance, if a large number of very similar systems must be changed, but each with minor variances, an autonomous approach may work not only faster, but more accurately, as

such repetitive tasks are often poorly performed by people – the tasks are simply too boring to keep one's attention.

The difficulties entailed in achieving autonomous change are equally clear: all the activities discussed above must be completely realized as executable processes, from data observation, to analysis, to planning, to deployment, to run-time system modification. Moreover all these executable processes, and all the information involved in their execution, must reside on the autonomous system. Pre-eminent in this information is the architectural model of the system. Note that with this on-board, and kept faithful to the implementation, the system is continuously self-describing.

In practical terms self-adaptive systems today are limited to rather simplistic situations, for which a set of rule-based adaptation policies can be formulated. As previously discussed, this is appropriate for systems where the types of adaptation needs can be anticipated and encoded in simple terms. Expanding the range of systems and types of change for which autonomous solutions can be developed is an area of active research.

According to IBM, "Autonomic computing is an approach to self-managed computing systems with a minimum of human interference. The term derives from the body's autonomic nervous system, which controls key functions without conscious awareness or involvement. Autonomic computing is an emerging area of study and a Grand Challenge for the entire I/T community to address in earnest."

The initial autonomic computing manifesto [127], as issued by IBM, focused attention on installation and management of IT infrastructure, such as corporate servers and networks, and their use in business processes. According to this manifesto there are at least eight key characteristics of autonomic systems:

1. "To be autonomic, a computing system needs to 'know itself' – and comprise components that also possess a system identity."
2. "An autonomic computing system must configure and reconfigure itself under varying and unpredictable conditions."
3. "An autonomic computing system never settles for the status quo – it always looks for ways to optimize its workings."
4. "An autonomic computing system must perform something akin to healing – it must be able to recover from routine and extraordinary events that might cause some of its parts to malfunction."
5. "A virtual world is no less dangerous than the physical one, so an autonomic computing system must be an expert in self-protection."
6. "An autonomic computing system knows its environment and the

"Autonomic Computing," IBM's Grand Challenge for the IT Industry

- context surrounding its activity, and acts accordingly.”
7. “An autonomic computing system cannot exist in a hermetic environment.”
  8. “Perhaps most critical for the user, an autonomic computing system will anticipate the optimized resources needed while keeping its complexity hidden.”

Clearly IBM’s vision for autonomic computing is consistent with the architecture-based approach to adaptation articulated in this chapter. Indeed, the first characteristic listed above is essentially a restatement of the requirement of maintaining an “on-board” model of a system’s architecture, as discussed in main body of the text.

**References:** [128, 150]

Autonomic Computing Conference <http://www.autonomic-conference.org/>.

#### 14.4 End Matter

There is little question that applications will be adapted and changed over their lifetime. The real question is how expensive and how difficult will it be to effect those changes? While “designing for change” and the use of encapsulation is an important principle for assisting with change, much more powerful and capable mechanisms are required for meeting contemporary adaptation needs. This chapter has presented such mechanisms:

- A conceptual framework for governing the entire adaptation process
- Architectural styles that assist with accommodating large-scale system change
- Specific techniques for assisting with the major tasks of adaptation: monitoring, analyzing, planning, and effecting.

If a system’s descriptive architecture and its prescriptive architecture are consistent, then adaptation can be orchestrated around changes to the architectural model. This approach, besides providing the intellectual tools for managing “ordinary” adaptation, opens the door to novel types of application evolution, such as wherein the architectural model is deployed with the application and adaptation processes on the target machine utilize the model in determining and carrying out changes.

software. To not adapt is to abandon the investment. To adapt cost-effectively is the challenge.

An architecture-based approach to adaptation offers:

- New opportunities for products/applications
- Better opportunities for maintaining deployed products
- Better opportunities for responding to customer enhancement requests
- Less downtime
- New opportunities for third-party enhancement, while maintaining control of intellectual property.

The concept behind the last bullet above is to expose parts of the architecture that enable third parties to add value through their proprietary extensions, but to do so without exposing the internals of components, or even allowing the third-parties to become aware of the existence of large portions of the primary architecture. This strategy appears to be successful in, for example, commercial image processing applications.

One risk of supporting adaptation is abuse based upon perceived ease. That is, if marketing, for example, is led to believe that the organization can effectively support product evolution “with ease”, then they may be less likely to carefully analyze new customer requests or to bundle requests for changes into meaningful packages.

#### 14.5 Review Questions

1. What are the fundamental causes or motivations for software adaptation?
2. What are the major activities of software adaptation?
3. For each of the major activities of adaptation, describe a technique that assists in performing that activity.
4. How can architectures be designed to make the task of third-party extension easier?

#### 14.6 Exercises

34. Consider the problem of modifying several of the lunar lander designs of Chapter 4 to serve as a Martian lander. Would the changes required be confined to components, or would connectors be involved?
35. Consider the problem of adapting the lunar lander designs of Chapter 4 to work by remote control. That is, instead of the lander having a pilot on board, the craft is unmanned and a pilot on Earth must control the

- descent. What type of changes would be required to the components? To the connectors?
36. Consider the challenges faced in adapting a planetary exploration vehicle, such as the Cassini mission to Saturn. What would be a suitable architectural style for supporting in-flight system adaptation? Would you have a kernel that is non-updatable? Why or why not?
  37. What degree of quiescence would be required in your answer to question 36 when performing an update? To what extent does your answer depend on the type of update (i.e. the degree of change involved)?
  38. What are the differences (if any) between software architectures that support dynamic adaptation and fault-tolerant architectures? What circumstances are the approaches suited for?
  39. Suppose you had optimized a connector in the implementation of a system for performance reasons and then need at some later date to modify the architecture. How would you approach adaptation of this system if the adaptation is performed off-line? What if the adaptation must be performed dynamically?
  40. Analyze the robotic architectures of Chapter 11 with respect to their ability to effectively accommodate changes such as requiring the robot to (a) perform a minor variation to an existing task, (b) utilize a new “tool”, such as a new robotic arm, to perform an entirely new task.
  41. Is pre-planned change really an instance of “dynamic architecture”? Why or why not? What should the litmus test be?
  42. (Research question) What is the role of dynamic adaptation (or just “adaptation”) in the context of software product families? When should adaptation of a member of a family be considered creation of a new product?
  43. (Research question) Does design of an application to support ease of adaptation conflict with the ability to assure that any given instance of the application performs its intended task? In general, does ease of adaptation conflict with analyzability?

## 14.7 Further Reading

Since change has accompanied software development from the outset of the field there is no shortage of literature discussing how to adapt software. Indeed, the entire “millennium bug”/Y2K problem was one massive effort in software adaptation. In that case, of course, the change being effected was extremely narrowly focused. Sadly, for some Y2K systems architecture changes were required since the two-digit fault was so implicitly part of the system’s design.

Stewart Brand’s book on change in physical architectures [27], discussed in the preceding text, is well-worth an extensive read, for it has numerous insights on adaptation that have correspondences in software adaptation.

If nothing else you will discover why you love some buildings and hate others.

Some of the earliest work in architectural approach to adaptation was performed at Imperial College by Jeff Kramer and Jeff Magee as part of the Regis [174, 203] and Conic projects [155]. Successive work with Darwin continues this theme [176].

Peyman Oreizy and colleagues are responsible for many of the key insights presented in this chapter, including the original conceptual model for the management of self-adaptive systems [215, 216] and the characterization of the architectural styles promoting adaptability presented in Section 0. Follow-on work from that includes approaches based on knowledge-based systems [93, 94]. Gomaa has explored the use of patterns to facilitate reconfiguration in [100], and addresses the issue of quiescence.

Many more references are available from the proceedings of the leading workshops in the field, which include the Workshop on Software Engineering for Adaptive and Self-Managing Systems and the Workshop on Architecting Dependable Systems.

## CHAPTER 15

**15 Domain-Specific Software Engineering**

Software systems differ in terms of their purpose, size, complexity, provided functionality, quality needs, intended usage, expected or required execution context, involved stakeholders and their concerns, level of criticality to system users, and so on. An argument can be made that this is precisely why software is difficult to develop. However, such differences across individual systems are not unique to software engineering. They can be found in any complex system and any engineering discipline.

As an example, consider two different products of modern engineering: airplanes and television sets. Both airplanes and televisions are complex systems, but their functionalities differ a great deal. They also have very different quality requirements. While it is certainly important for a television to function reliably, in the case of airplanes reliability is absolutely critical and can be a matter of life-and-death. Travelers expect airplanes to be robust in the face of atypical situations: storms; turbulence; loss of engine power, electrical power, or cabin air pressure; physical damage to the aircraft; and so on. On the other hand, consumers understand when, say, a sudden electrical power surge damages their TV set, and are content either to wait patiently for several days for the TV to be repaired or simply to purchase a new one. People expect that an airplane may be in use for decades, and that it will need to be refurbished and upgraded during that time. They do not have the same expectations of a television.

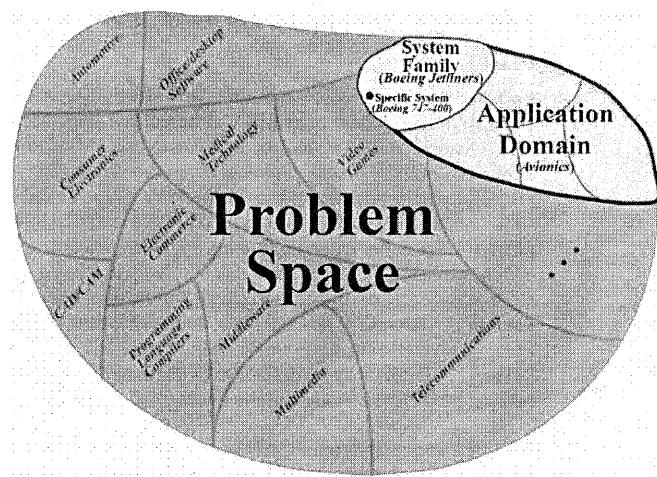
Airplanes and televisions are products of (very) different engineering problem *domains*. As a result of these differences, the respective skill sets of the engineers working in the two domains are also likely to be specialized and very different: it would be unrealistic to expect an electrical engineer working on airplanes to be able to switch to building televisions without (perhaps significant) re-training; and most people would probably feel very uneasy if they found out they were flying on an airplane built by engineers whose expertise was in constructing televisions. There are many obvious reasons for this, of which the main one is that the problems solved in the two domains require different principles, techniques, processes, and tools, which are carefully, and

separately, honed over years or decades. Simply put, the two problem domains demand different solutions, and those developed for one domain are highly unlikely to fit the other.

Each application domain may further have several *sub-domains*. For example, in the context of avionics, different sub-domains may encompass rotary-wing aircraft (i.e., helicopters) versus fixed-wing aircraft (i.e., airplanes), military versus commercial aircraft, jet-engine versus propeller-engine aircraft, and so on. Within a single domain or one of its sub-domains, organizations often focus on constructing *populations* of related systems. For example, Boeing engineers work on a wide variety of commercial and military aircraft that are likely to share some engineering characteristics. More easily recognized are the more closely related *families* of systems, or *product lines*, that exist within those populations. In the case of Boeing, an example would be the 7x7 family of passenger airliners. A family may be defined even more narrowly, for example, to encompass different models of the Boeing 747 jumbo-jet.

Given the above description, it is reasonable to expect that, even within the domain of avionics, an engineer working on rotary-wing aircraft may have different skills from his colleagues working on fixed-wing aircraft. Likewise, an engineer building a military jet may have different experience and expertise from an engineer building a commercial airliner. Even more specifically, an engineer working within Boeing's commercial airliner division may approach certain aspects of his craft differently from his counterpart at Airbus: there is a great deal of overlap regarding *how* different members of the Boeing 7x7 family of passenger jets are constructed; while many of the underlying principles are the same, the comparable Airbus airliners are likely to have been designed and built differently.

Figure 15-1. Engineers construct systems within many problem domains (e.g., video games, middleware, automotive, avionics, etc.). Each domain may comprise one or more sub-domains (e.g., fixed-wing vs. rotary wing aircraft, commercial airliners, military jets, etc. within the avionics domain—elided from the figure for simplicity). Within each domain there may be different system families (e.g., Boeing 7x7 commercial airliners). Finally, within each family, there are many different systems (e.g., Boeing 747-400).



An analogous narrowing of the problem scope, and specialization of the engineers' skills, can be observed in other domains. For example, in the consumer electronics domain, a Philips engineer is likely to have somewhat different skill sets from, say, a Sony engineer. As another example, within the automotive domain, a General Motors engineer may be trained specifically to apply his technical expertise to the broad population of GM vehicles, or more narrowly to, say, the family of Cadillacs. Figure 15-1 illustrates this progressive narrowing of the problem scope and the resulting growth in commonality among systems.

As with any profession, software engineers have basic skills, techniques, guidelines, tools, and so on that are applicable independent of the target domain. Separation of concerns, modularity, object-orientation, design patterns, UML, Java, CORBA, and so on comprise a common "toolbox" at the disposal of software engineers. It would not be unfair to think of these as equivalent to, say, Maxwell's laws, soldering irons, capacitors, resistors, and so on, which are at the disposal of an electrical engineer.

However, these basic tools and principles are only a rudimentary foundation for the construction of complex systems. They neither attempt to leverage the useful properties of a given problem domain, nor do they help to identify and exploit the similarities that are likely to exist across systems in a given family. It would be too difficult, error-prone, and costly

to attempt to build every software system using only these primitive tools. In the early days of computing this is exactly what software engineers were forced to do. They had little or no knowledge about building software, especially within particular domains, to help them, so they had to develop software systems from "first principles".

The situation today is very different. Large amounts of engineering knowledge have been acquired through extensive experience (and costly failures) in many domains. Within these domains, many product populations and product lines have been developed and evolved. By leveraging knowledge from these experiences, engineers can build subsequent systems within the same domain or family more quickly, cheaply, and reliably. To use our earlier analogy, while the ability to build a television may not translate to the ability to build an airplane, the ability to build one airplane imparts a large amount of information about how to build another.

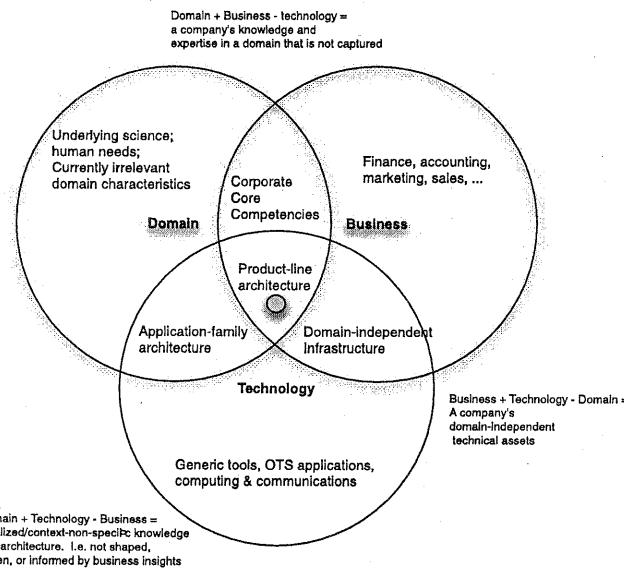
Domain-specific software engineering (DSSE) is the name given to an approach to software engineering that is characterized by extensively leveraging existing domain knowledge. DSSE is a powerful strategy because:

- The requirements for a system can be divided into those common across the application domain and those unique to the system.
- The common requirements can be tied to the existing canonical solutions, allowing developers to focus on the remaining subset.
- The system implementation, testing, and maintenance are thereby simplified because of the already existing reusable software "assets" (e.g., engineering knowledge, design models, implemented subsystems, test suites, deployment scripts, and so on).
- Development activities are simplified through software tools and environments that are specialized for the domain.
- Any concerns are more easily communicated among the system's stakeholders because of the shared understanding, experience, and even terminology, which may have been developed incrementally and may be specific to the application domain.

As we will elaborate in this chapter, DSSE combines insights from three principal areas:

1. the *domain*, which scopes the discourse, the problem space, and the solution space;
2. *business goals*, which motivate the work and help engineers decide why they are doing what they are doing; and

3. *technology*, which is used to facilitate development and reuse of domain- and business-specific assets.



**Figure 15-2.** Domain-specific software engineering requires organizations and engineers to leverage different aspects of three inter-related areas: domain, business, and technology.

The respective roles of and relationships among these areas are depicted in Figure 15-2. This figure provides a conceptual basis for the remainder of this chapter. It allows us to define, relate, and explain appropriately two key facets of DSSE: domain-specific software architectures (DSSA), and product families, also referred to as product lines (PL). Even though they are closely related, these two areas of software engineering to date have received mostly separate treatments in the literature.

This chapter will introduce and discuss the DSSE concepts foreshadowed above, with a particular focus on the role of software architecture in DSSE. By the end of the chapter, the reader will have an understanding of how DSSE is different from ordinary architecture-based software engineering, what its benefits are, what the relationship is between DSSAs and PLs, and how to apply the resulting concepts to capture explicitly and effectively architectural solutions that span multiple systems across a domain or, more narrowly, across a system family.

#### Outline of Chapter 15

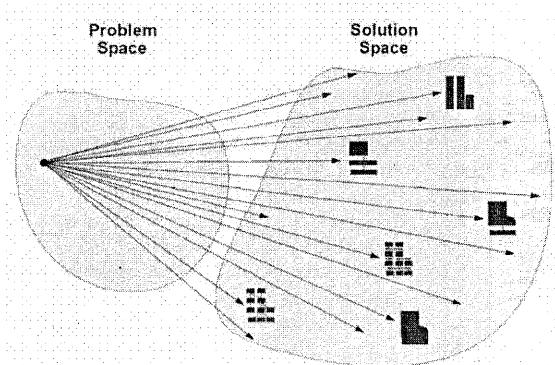
<b>15 Domain-Specific Software Engineering</b>
15.1 Domain-Specific Software Engineering in a Nutshell
15.1.1 Similar Problems, Similar Solutions
15.1.2 Viewing DSSE through the Prism of Domain, Business, and Technology
15.2 Domain-Specific Software Architecture
15.2.1 Domain Knowledge
15.2.2 Canonical Requirements
15.2.3 Canonical Solution Strategies—Reference Architectures
15.2.4 Product Lines and Architecture
15.2.5 Product-Line Concepts
15.2.6 Specifying the Architecture of a Product Line
15.2.7 Capturing Variations over Time
15.2.8 Using Product Lines as Tools for What-If Analysis
15.2.9 Implementing Product Lines
15.2.10 Unifying Product Architectures with Different Intellectual Heritage
15.2.11 Organizational Issues in Creating and Managing Product Lines
15.3 DSSAs, Product Lines, and Architectural Styles
15.4 DSSE Examples
15.4.1 Koala and Consumer Electronics
15.4.2 Software Defined Radios
15.5 End Matter
15.6 Review Questions
15.7 Exercises
15.8 Further Reading

## 15.1 Domain-Specific Software Engineering in a Nutshell

Before we go on to the specifics of DSSAs and PLs, let us provide a brief context for them.

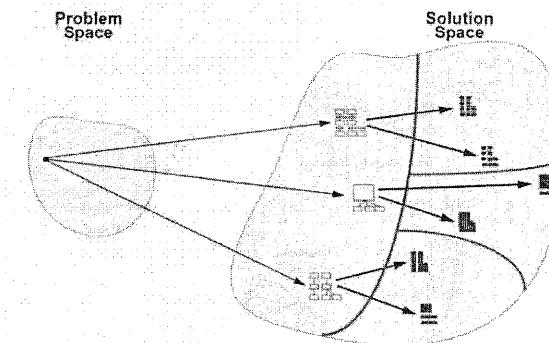
### 15.1.1 Similar Problems, Similar Solutions

**Figure 15-3.** A deliberately simplified view of traditional software development: Any given software development problem can be solved in a large number of different ways.



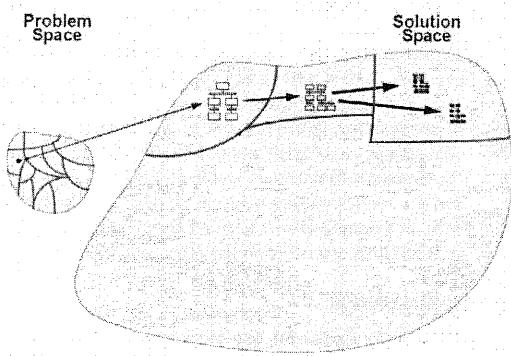
For the purpose of illustrating our discussion, we show a highly simplified view of traditional software development in Figure 15-3: A team of software engineers is typically given a description of a problem with which they are tasked. That description may be detailed, or it may be cursory; it may be written down precisely, or it may be stated verbally (and ambiguously) by a human customer or prospective user; the description may be relatively complete, or it may emerge incrementally during the development process. In any case, the principal task of the software engineers is to find a way of taking the problem description, which exists in the *problem space*, and mapping it to a software system, which exists in the *solution space*. Doing so in general is difficult because the two spaces usually are characterized by different concepts, have different terminologies, and exhibit different properties. Doing so is also difficult because, in general, there are often many possibilities for addressing a given software requirement, ranging from the programming language in which the requirement will be implemented, to the code-level constructs used to realize the requirement, to the hardware platform on which it will execute, to the different ways of modularizing the system (including choosing not to modularize it at all), and so on. This is, in part, why historically it has been such a challenge for developers to ensure desired properties in software systems: too many choices without a clear indication of which choice works best, and why.

**Figure 15-4.** A deliberately simplified view of architecture-based software development: Any given software development problem can be solved by a finite number of software architectures.



Software architecture-based development addresses this problem in part by elevating the discourse to a higher plane with fewer choices: What are the principal components needed for the given system? What are their interactions? What are their compositions into system configurations that effectively solve the problem at hand? Figure 15-4 depicts this approach to system development. Again, the picture is deliberately over-simplified to illustrate the point: a problem will often have a more constrained number of software architectural solutions that are known to be effective for solving it. In turn, each of those architectures will have a comparatively smaller number of possible implementations (for reasons that have already been discussed in the preceding chapters).

**Figure 15-5.** A deliberately simplified view of DSSE: Some software development problems belong to specific classes of problems for which known (partial) architectural and implementation solutions exist. Those partial architectures are then tailored to the specific problem at hand and implemented using well-understood techniques.



Still, the task of selecting the appropriate software architecture and implementing it is anything but trivial. In many ways, this problem only interposes one additional level of indirection into the problem that software engineers faced in the past. This is where DSSE takes a markedly different approach, as depicted in Figure 15-5: Instead of primarily attacking the solution space, DSSE is guided by the observation that certain *problems* belong to specific, well-defined problem classes, or *domains* (recall Figure 15-1). That is, these problems share a number of characteristics that allow engineers to attack them in similar ways. Within each domain, effective (partial) architectural solutions can be identified and documented. These solutions are known as *reference architectures*. Instead of developing new architectures for each new problem in the domain, solutions can be derived by tailoring the reference architecture. Furthermore, the commonalities across the different problems in the same domain allow engineers to develop solid intuitions about a system before it is built, evaluate their solutions in a principled and often rigorous manner, and leverage a large number of powerful tools for generating and evaluating system implementations. All of the resulting activities, techniques, and tools are aided by their relatively narrow, well-defined focus and scope.

### 15.1.2 Viewing DSSE through the Prism of Domain, Business, and Technology

As argued in the chapter's introduction and depicted in Figure 15-2, three principal concerns of DSSE are domain, business, and technology [190]. The prominence of each of the three concerns, and their exact mix, will differ across organizations and projects. Those differences have clear implications on the organizations and projects concerned, as well as on the

stakeholders, processes, and ultimately products. We discuss each area in the diagram from Figure 15-2 in more detail below.

**Domain:** The domain, independent of business and technology concerns, establishes a problem space. It has defined characteristics, a vocabulary, a motivation (why this domain exists), and so on. This area will be further expanded below, in the “Domain Model” section.

**Business:** Business, independent of any domain or technology concerns, is largely concerned with human goals: improving people’s quality of life through the creation of new products, attaining money, power, notoriety, and so on. These goals motivate people to solve problems. Note that this is not meant to imply that domain-specific software must be sold or otherwise developed for the purpose of attaining monetary profits. However, the goal of using DSSE is to optimize certain aspects of software engineering: reducing cost or time to develop, improving the quality of products in the market (even open-source products), and so on.

**Technology:** Technology, independent of a domain or business goals, comprises tools, applications, reusable components, infrastructure, and methods that can be applied generally. In this sense, technology could be characterized as “solutions without problems”.

**Domain + Business:** When business goals are applied to a particular domain, expertise and core competencies emerge. Business organizations specialize their skills to optimize them for particular domains: building televisions or airplanes, for example.

**Business + Technology:** Regardless of the domain(s) in which it operates, a business organization will acquire and develop technologies that are relevant to its overall goals but can be applied to many domains. For example, any software development organization will undoubtedly have an infrastructure containing compilers, operating systems, networks, office applications, and so on that does not apply specifically to any domain.

**Domain + Technology:** This intersection contains tools, methods, and even architectures that are specifically applicable to a particular domain, but are independent of any particular business goal. For example, a programming language and compiler that are specifically developed for building aircraft software would fall into this category.

**Domain + Business + Technology:** This is the core of domain-specific software engineering: Business goals motivating the identification and creation of a solution in the problem space of a domain, facilitated by the use of technology.

We have outlined the various concepts and interactions that comprise domain-specific software engineering. Now, we will examine how software architecture can be leveraged and specialized for application in the context of DSSE. We will study two key architecturally-relevant areas of DSSE: domain-specific software architectures and product lines.

## 15.2 Domain-Specific Software Architecture

A domain-specific software architecture (DSSA) [42, 286, 288, 290] comprises a codified body of knowledge about software development in a specific application domain. Hayes-Roth [114] provides a useful operational definition of DSSA:

**Definition.** A domain-specific software architecture (DSSA) comprises:

- a reference architecture, which describes a general computational framework for a significant domain of applications;
- a component library, which contains reusable chunks of domain expertise; and
- an application configuration method for selecting and configuring components within the architecture to meet particular application requirements.

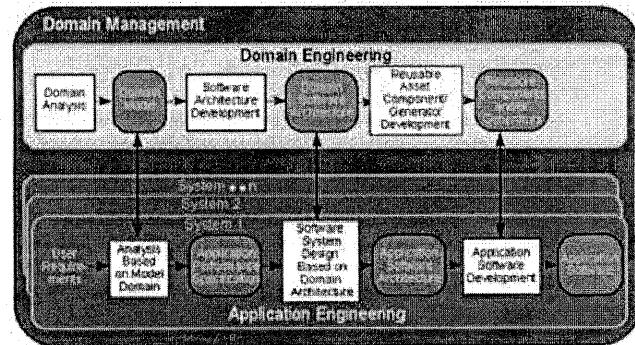


Figure 15-6. Overview of the DSSA process and managed artifacts.

*@@Borrowed from SEI's FODA; may be replaced with a similar diagram.*

Figure 15-6 provides an overview of the DSSA-centric software development process. In addition to the usual *application engineering* activities in which developers engage, DSSAs involve a number of *domain engineering* activities. These activities result in models of the application domain's relevant entities, their characteristics, and their relationships; definitions of the key terminology; canonical requirements; design- and implementation-level solutions that are reusable across

systems in the domain; and tool support specialized to aid development within the domain.

This body of assets does not come for free. Instead, it is built over time, as engineers amass experience (both good and bad) of building individual systems within a domain and try to generalize that experience for use in future systems. In the remainder of this section we will discuss the characteristics of application domains and domain models, the requirements that remain stable and those that change within a domain, and the corresponding solution strategies. We will illustrate the discussion with an example DSSA derived from the different Lunar Lander architectures discussed in the preceding chapters.

### 15.2.1 Domain Knowledge

As we have discussed, one of the main concerns of domain-specific software engineering is the problem domain itself. In order to exploit effectively the properties of the domain, its key characteristics must be captured in some fashion. This section will discuss the key elements of a domain model and illustrate them with the Lunar Lander example.

Simply put, a *domain model* [17] is a representation of what happens in an application domain. This includes the *functions* being performed, the *objects* (also referred to as *entities*) performing the functions and those on which the functions are performed, and the *data* and *information* flowing among the entities and/or functions. In the parlance of the preceding section, a domain model deals with the problem space. Therefore, the above terms are used in their original sense (e.g., function as a mathematical notion with precisely defined properties, or as an operation performed on or by a device “living” in the domain), rather than in the sense that as software engineers we typically assign to them (e.g., function as a method without side effects in a C++ program).

If we take avionics as an example domain, the functions of interest would be aircraft take-off, landing, taxiing, flying, pitch, roll, yaw, fueling, refueling (possibly in-flight), maintenance, and so on. Data and information flowing among these functions would be various pilot commands, instrument signals, warnings, status check messages, fuel consumption rates, data collected for the “black boxes”, and so on. The entities in the domain would include the flight instruments, the aircraft’s rudder and wing flaps, the fuel tanks, the fuel transferred into the tanks during fueling and from the tanks to the engine during flight, the hydraulic fluids used to control the aircraft, and so on. It is this type of terminology, entities, their relationships, and operations on them that go into constructing a domain model.

Note that nothing in the above, albeit very brief and informal, domain description belies the fact that a significant portion of a given avionics system's functions, data, and entities will eventually be reified in software. The fundamental objective of a domain model is two-fold:

1. A domain model standardizes the given problem domain's *terminology* and its *semantics*. Together, the terminology and semantics are referred to as the domain's *ontology*.
2. A domain model provides the basis for standardized descriptions of problems to be solved in the domain.

For example, *yaw* is a term used in avionics to refer to an aircraft's rotation about an axis that is perpendicular to the aircraft's horizontal plane (that is, its wings) and goes through the aircraft's center of gravity. We would, of course, also have to define what a center of gravity is, and then possibly any other terms needed to clarify its definition, and so on, until all the terms related to yaw are explained using the appropriate domain-specific terminology. Yaw is produced by moving the aircraft's rudder.

Note that, while *yaw* is a widely known term because of the popularity and ubiquity of flight in today's world, nothing really prevents us from using a different term to describe this same concept in another problem domain. For example, we might call the analogous movement of a flat-panel television screen *left-right rotation*. Similarly, we can use this same term to describe a different concept in another problem domain (although in this case we would risk confusing matters given the broad familiarity with this particular term and its above-defined meaning).

A domain model is a product of context analysis and domain analysis. *Context analysis* is the activity whereby the boundaries of a domain are defined, and the relationships of the entities inside the domain to those outside it identified and captured. This is an important activity that sometimes remains overlooked, since DSSE focuses primarily on things *within* a domain, rather than the bounds of the domain or the relationship between things inside and outside the domain.

*Domain analysis* can be defined as the activity of identifying, capturing, and organizing the *domain assets*, that is, the objects, operations, and data recurring across a class of similar systems within an application domain. Domain analysis results in a description of the domain assets using a standardized vocabulary. Its goal is to set the foundation of making the assets usable and reusable when solving new problems within the domain. For example, *yaw* is a usable asset if it is described in a manner that an avionics (software) engineer can find it easily and understand its meaning unambiguously whenever needed. *Yaw* is *reusable* if it describes an

operation of all, or at least most, aircraft within the domain (for example, large passenger airplanes). Note that this level of reuse, while clearly important to multiple projects conducted by an engineering organization, including its software engineering divisions, has little if anything to do with code.

A domain model will usually comprise several pieces of information that together present a useful picture of the domain assets and their interrelationships. These models can be grouped into four categories:

- domain dictionary;
- information model;
- feature model; and
- operational model.

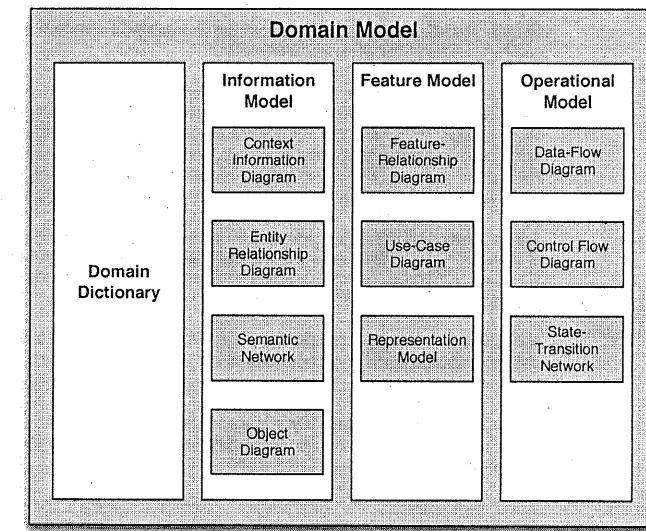


Figure 15-7. Elements of a domain model.

The different models and a broad cross-section of their associated diagram types are shown in Figure 15-7. We will now discuss each of them in more detail.

#### Domain Dictionary

A domain dictionary represents the identification and definitions of terms used in the domain model. These terms may be widely used and

understood outside the domain, in which case the goal of including them in the domain dictionary may be to define them carefully and avoid any inconsistencies and ambiguities in their usage. On the other hand, the terms may be specialized, or even invented for the sole purpose of fostering human stakeholders' communication and understanding within the domain. The domain dictionary should be updated over time with new terminology and with new or clearer understandings of existing concepts. A domain dictionary also becomes an indispensable tool for training new engineers working within the application domain.

**Command/Service Module (CSM):** the section of the spacecraft that orbits the moon; the Lunar Module undocks from the CSM and lands, re-docking with the CSM for the return trip to Earth.

**Descent Propulsion System (DPS):** a system of the Lunar Module that includes fuel tanks and descent engine

**DSKY:** Display and Keyboard Unit of the spacecraft's onboard computer; the user interface of the on-board computer

**Guidance, Navigation and Control System (GN&C):** a system on the Lunar Module responsible for collecting and calculating data (including position, altitude, and velocity) to aid navigation and to achieve a specified trajectory. The two on-board computers are part of this system: Primary Guidance and Navigation System (PGNS) and Abort Guidance Section (AGS). Independent of the PGNS, the AGS acts as a backup in the event that PGNS malfunctions.

**Lunar Module (LM):** this is the portion of the spacecraft that lands on the moon. It consists of two main parts: the Ascent Stage (which holds the crew cabin) and the Descent Stage, which contains thrusters used for controlling the landing of the LM.

**Reaction Control System (RCS):** a system on the Lunar Module responsible for the stabilization during lunar surface ascent/descent and control of the spacecraft's orientation (attitude) and motion (translation) during maneuvers

#### Vertical velocity (see also One-dimensional motion):

For a free-falling object with no air resistance, ignoring the rotation of the lunar surface, the altitude is calculated as follows:

$$y = \frac{1}{2} * a * t^2 + v_i * t + y_i$$

$y$  = altitude

$a$  = constant acceleration due to gravity on a lunar body  
(see Acceleration for sample values)

$t$  = time in seconds

$v_i$  = initial velocity

$y_i$  = initial altitude

When thrust is applied, the following equation is used:

$$y = \frac{1}{2} * (a_{burner} - a_{gravity}) * t^2 + v_i * t + y_i$$

$y$  = altitude

Figure 15-8. Partial domain dictionary for a Lunar Lander DSSA.

$a_{burner}$  = constant acceleration upward due to thrust

$a_{gravity}$  = constant acceleration due to gravity on a lunar body  
(see Acceleration for sample values)

$t$  = time in seconds

$v_i$  = initial velocity

$y_i$  = initial altitude

Figure 15-8 shows a partial domain dictionary from a hypothetical Lunar Lander DSSA.

#### Information Model

An information model is actually a collection of multiple models that may be used in different organizations and different DSSAs. The information model is a result of context analysis and information analysis. As discussed above, context analysis results in defining the boundaries of the domain and preserves information that may be otherwise implicit and scattered across many different systems and their artifacts. Information analysis then takes the result of context analysis (that is, the contours of the domain) and represents the intra-domain knowledge explicitly in terms of domain entities and their relationships.

The information model ensures that the DSSA employs appropriate data abstractions and decompositions. Different elements of the information model are used by at least three types of stakeholders.

1. Requirements engineers use the information model as an aid in precisely specifying the reference requirements, that is, the requirements common across the applications in the DSSA (see the "Canonical Requirements" section below for a detailed discussion of reference requirements). They also use the information model to relate appropriately the application-specific requirements to the reference requirements.
2. Software architects use the information model to identify and relate appropriately the modules in the software system in the manner that reflects the characteristics of the domain, the interfaces exported by those modules, the data exchanged among them, and the mechanisms by which and constraints under which data is exchanged. This activity results in a reference architecture (see the "Canonical Solutions" section below for a detailed discussion of reference architectures). Software architects also use this information to relate application-specific architectures and designs to the reference architecture.
3. Software system maintainers use the information model to understand the manner in which any given application in the DSSA

addresses problems. This enables them to relate properly the system maintenance and evolution requirements to the reference requirements and application-specific requirements, and to relate their proposed realization in the system to the reference architecture and application-specific architecture.

An information model usually consists of one or more of the below types of diagrams:

*Context Information Diagram* captures the high-level data flow between the major entities in the system, their relationship to the entities outside the system (as well as outside the domain), as well as any data that is assumed to come from external sources.

For example, in the Lunar Lander DSSA, the information exchanged among the spacecraft's sensor, actuator, and computer are part of the context information diagram. At the same time, the topology of the moon's (or planet's) surface on which the spacecraft is landing is considered to be outside the domain.

### Context Diagram

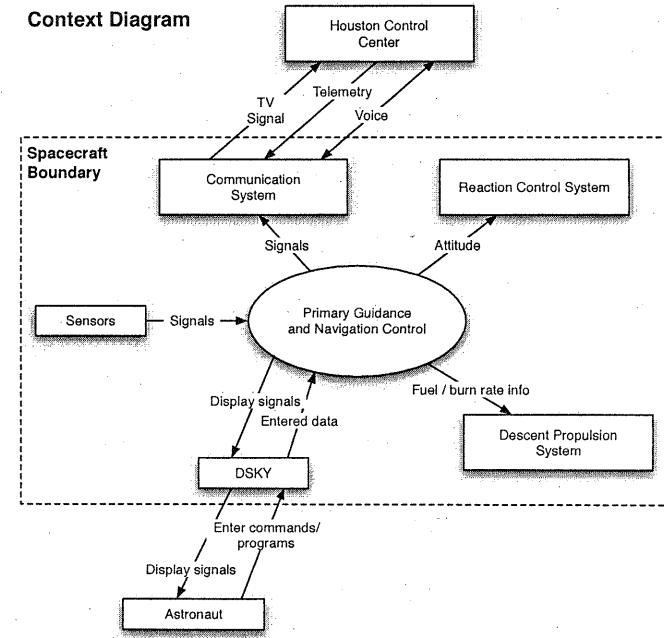


Figure 15-9. Example context information diagram from the Lunar Lander DSSA.

An example context information diagram from the Lunar Lander DSSA is shown in Figure 15-9.

*Entity/Relationship (ER) Diagram* captures aggregation (“a-part-of”) and generalization (“is-a”) relationships among the entities within the domain. For example, in the Lunar Lander DSSA, fuel level is “a-part-of” the spacecraft entity, while a given thruster “is-a” Lunar Lander actuator.

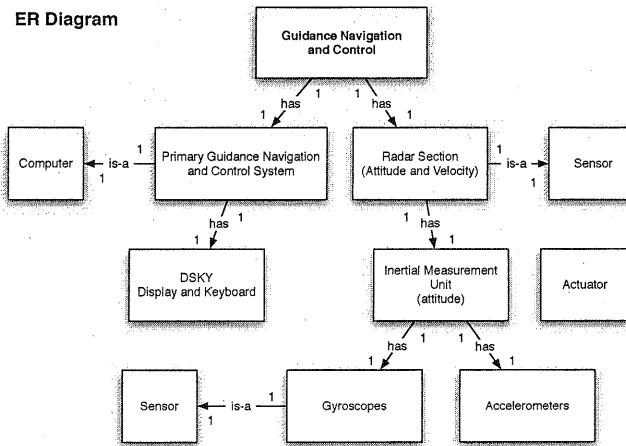


Figure 15-10. Example ER diagram from the Lunar Lander DSSA.

An example ER diagram from the Lunar Lander DSSA is shown in Figure 15-10.

Object Diagram identifies the objects in the application domain, rather than in the software. In other words, the object diagram describes entities (that is, components) in the problems space; the solution-space components used to realize the problem-space entities will be captured in the reference architecture, discussed below. The object diagram captures the attributes and properties of each object, as well as their interdependencies and interactions with other objects in the domain.

**Object Diagram**

Object	Attributes	Operations
Landing Radar	Altitude Velocity	Sense Altitude (height) Sense Velocity
Descent Engine	Throttle Level Nozzle Direction	Set Throttle Level Change Nozzle Direction (Gimbal) Turn On / Off
Thrust Engines	Firing Mode Altitude Translation	Set Firing Mode to pulse or continuous Change Spacecraft Attitude Change Spacecraft Translation

Figure 15-11. Example object diagram from the Lunar Lander DSSA.

An example object diagram from the Lunar Lander DSSA is shown in Figure 15-11.

#### Feature Model

The feature model is also in fact a collection of several models. A feature model results from feature analysis. The goal of feature analysis is to capture and organize a customer's and/or end-user's understandings and expectations of the overall (shared) capabilities of applications in a given domain. The feature model is considered to be the chief means of communication between the customers and the developers of new applications. The feature model explicitly delineates the commonalities and differences among systems in the domain. Examples of features include: function descriptions, descriptions of the mission and usage patterns, performance requirements, accuracy, time synchronization, and so on [148]. Such features are meaningful to the end users and can assist the engineers in the derivation of DSSA that will provide the desired capabilities.

Features may be defined as mandatory, optional, or variant. Mandatory features are expected to recur across all systems in the domain. In the case of the Lunar Lander system, *Compute Height* is a mandatory feature: any implementation of the Lunar Lander must be able to continuously compute the spacecraft's height. Optional features are those that are identified as useful for a subset of the systems within the given DSSA. For example, *Get Burn Rate* is an optional feature: some versions of the Lunar Lander

are able to ask the system user for the preferred fuel consumption rate. Finally, variant features exist in most (or all) systems within a DSSA, but slightly differ depending on the values of one or more parameters. For example, *Compute Velocity* is a variant feature within the Lunar Lander DSSA, whose exact realization may depend upon the size and mass of the spacecraft as well as the size, mass, and atmosphere of the celestial body onto which the spacecraft is landing.

The feature model also encompasses several types of diagrams, which are discussed below. As with the information model, the architects developing the feature model for a particular DSSA would decide which of these diagrams best suit their needs. They might also choose other types of similar diagrams. For example, Software Engineering Institute's Feature Oriented Domain Analysis (FODA) approach advocates the use of semantic networks [148] in feature modeling.

*Feature Relationship Diagram*<sup>17</sup> describes the overall mission or usage patterns of an application. It captures the major features and their decomposition into sub-features. This model can also include any quality requirements associated with individual features such as dependability, security, performance, accuracy, real-time requirements, synchronization, and so on (recall Chapters 12 and 13).

#### Feature Relationship Diagram – Landing Phase

**Mandatory:** The Lunar Lander must continually read altitude from the Landing Radar and relay that data to Houston with less than 500 msec of latency. Astronauts must be able to control the descent of the Lunar Lander using manual control on the descent engine. The descent engine must respond to control commands in 250msec, with or without a functioning DSKY...

**Optional/Variant:** Lunar Lander provides the option to land automatically or allow the crew to manually steer the spacecraft.

#### Quality Requirements:

**Real-time requirements:** The thrusters and the descent engine must be able to respond to commands from the computer system in real-time.

**Fault tolerance:** Lunar Lander must be able to continue in its flight-path even when the main computer system (Primary Navigation Guidance & Control) goes down. Lunar Lander must be able to maintain system altitude even when one of

Figure 15-12. Example feature relationship diagram from the Lunar Lander DSSA.

<sup>17</sup> Feature model model is sometimes also referred as “context model”, and the feature relationship diagram “context diagram”. We deliberately refrain from using “context” in this setting in order to avoid confusing matters with the context diagram in the information model.

the thrusters and propellant supplies goes down in the Reaction Control System. Lunar Lander's computer system must function properly after a restart (restart protection).

An example feature relationship diagram from the Lunar Lander DSSA is shown in Figure 15-12.

*Use-Case Diagram* captures the usage scenarios in the system. Use cases have become prevalent with the introduction of the Unified Modeling Language (see Chapter 16). Use-case diagrams are elicited from domain experts, system customers, and/or system users, and encompass the manner in which a feature is expected to be used, as well as control- and data-flow among multiple features.

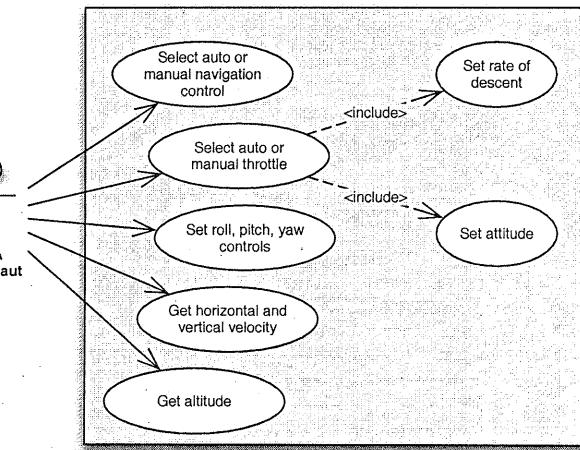
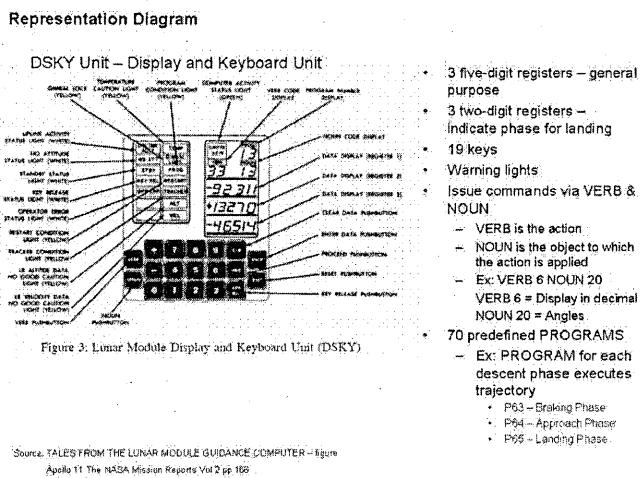


Figure 15-13. Example use-case diagram from the Lunar Lander DSSA.

An example use-case diagram from the Lunar Lander DSSA is shown in Figure 15-13.

*Representation Model* describes how information is made available to a human user. In other words, the representation model details what the appropriate user interfaces are for the systems within the DSSA. This model also captures the information produced for another application: what kinds of input and output capabilities are available, and what is the expected, common format for the exchanged information?



**Figure 15-14.** Example representation model from the Lunar Lander DSSA.

An example partial representation model from the Lunar Lander DSSA is shown in Figure 15-14.

## Operational Model

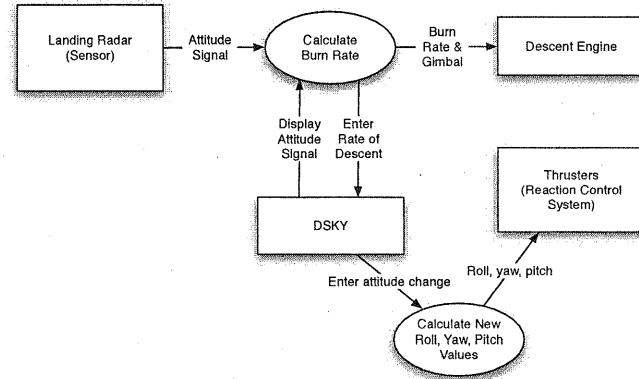
The operational model is the foundation upon which the software designer begins the process of understanding (1) how to provide the features for a particular system in a domain, and (2) how to make use of the entities identified in the resulting domain model. Operational model identifies the key operations (i.e., functions) that occur within a domain, the data exchanged among those operations, as well as the commonly occurring sequences of those operations. In other words, operational model represents *how* applications within a domain work.

Operational model is a result of operational analysis, which identifies the commonalities as well as differences in control-flow and data-flow among the entities in a domain. The domain-wide entities identified in the information and feature models, discussed above, form the basis for the operational model: information model captures the data exchanged by the operations, while the feature model captures the operations themselves. The control- and data-flow of each individual application within the DSSA can be instantiated or derived from the operational model.

Three representative types of diagrams used within the operational model are discussed below.

Data-Flow Diagrams focus explicitly on the data exchanged within the system, with no notion of control.

## Data Flow Diagram



**Figure 15-15.** Example data-flow diagram from the Lunar Lander DSSA.

An example data-flow diagram from the Lunar Lander DSSA is shown in Figure 15-15.

Control-Flow Diagrams, on the other hand, focus on the exchange of control within the system, without regard for data.

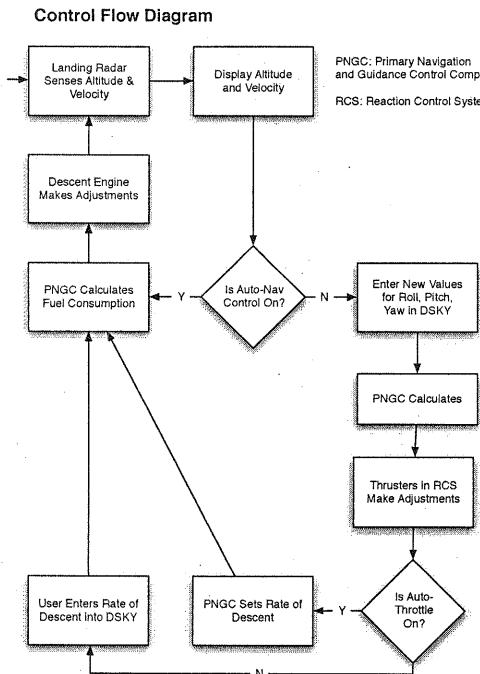


Figure 15-16. Example control-flow diagram from the Lunar Lander DSSA.

An example control-flow diagram from the Lunar Lander DSSA is shown in Figure 15-16.

State-Transition Diagrams model and relate the different states that the entities in the domain will enter, events that will result in transitions between states, as well as actions that may result from those events.

### State Transition Diagram

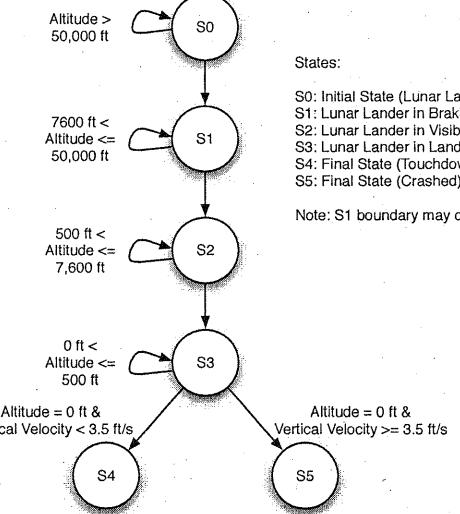


Figure 15-17. Example state-transition diagram from the Lunar Lander DSSA.

States:  
 S0: Initial State (Lunar Lander in Descent Orbit)  
 S1: Lunar Lander in Braking Phase  
 S2: Lunar Lander in Visibility Phase  
 S3: Lunar Lander in Landing Phase  
 S4: Final State (Touchdown)  
 S5: Final State (Crashed)

Note: S1 boundary may differ from 7,600 ft.

An example state-transition diagram from the Lunar Lander DSSA is shown in Figure 15-17.

### 15.2.2 Canonical Requirements

A critical element of a DSSA is the canonical or *reference* requirements. These are requirements that apply across the entire domain captured by a DSSA. In that sense, reference requirements will be incomplete, since they must be general enough to capture the variations that occurring across individual systems, and since individual systems will additionally introduce their own requirements. However, reference requirements directly facilitate the mapping of the requirements for each system within a given domain to the canonical domain-specific solution (discussed in the next section).

Similarly to the requirements for any software system, the starting point for reference requirements is the customer needs statement. This statement is generic, and is applicable to any system in the domain. Since a DSSA is an exercise in generalization from specific experience, the customer needs statement may emerge over time, from similar such statements that were specific to individual systems constructed previously.

within the domain. The customer needs statement identifies the functional requirements for the DSSA at a high level of abstraction. It is usually informal, ambiguous, and incomplete. It is a starting point for deriving (reference) requirements, but it is not the same as reference requirements.

*A family of related systems is needed that*

1. *supports the Lunar Lander video game for different platforms (e.g., PC, Mac, Pocket PC, cell phone, etc.),*
2. *supports different user interfaces, from simple textual to a sophisticated 3-D GUI,*
3. *runs on a single machine or is decentralized across a network,*
4. *works in a single-user or multi-user competition mode, and*

*supports different variations (e.g., only landing from a given height, first entering orbit and then landing, landing on different types of terrain, landing on different types of celestial bodies, etc.).*

Figure 15-18. Example customer needs statement from the Lunar Lander DSSA.

As an example, Figure 15-18 shows a partial customer needs statement for the Lunar Lander DSSA.

Reference requirements are then derived from the customer needs statement as well as the requirements of the individual legacy systems within the domain. The reference requirements contain the defining characteristics of the problem space. These are the *functional requirements*. Reference requirements also contain limiting characteristics (that is, constraints) in the solution space. These are the *non-functional requirements* (e.g., security, performance, reliability), *design requirements* (e.g., architectural style, user interface style), and *implementation requirements* (e.g., hardware platform, programming language).

Similarly to the feature model discussed above, reference requirements must distinguish among three types of requirements:

1. *Mandatory requirements* are applicable to all systems in the domain.
2. *Optional requirements* are known to be applicable to a certain set of systems within the domain.
3. *Variable requirements* are application-specific, and may be unknown at the time the DSSA, and more specifically reference requirements, are formulated.

In general, each requirement—whether functional, non-functional, design, or implementation requirement—can be of any one of the three types (mandatory, optional, or variable).

Figure 15-19. Example reference requirements from the Lunar Lander DSSA.

**Mandatory**

- *Must display the current status of the Lunar Lander (horizontal and vertical velocities, altitude, remaining fuel)*
- *Must indicate points earned by player based on quality of landing*

**Optional**

- *May display time elapsed*

**Variant**

- *May have different levels of difficulty based on pilot experience (novice, expert, etc)*
- *May have different types of input depending on whether*
  - *Auto Navigation is enabled*
  - *Auto Throttle is enabled*
- *May have to land on different celestial bodies*
  - *Moon*
  - *Mars*
  - *Jupiter's moons*
  - *Asteroid*

We provide examples of all three requirements types for the Lunar Lander DSSA in Figure 15-19.

### 15.2.3 Canonical Solution Strategies—Reference Architectures

When business goals and technology are applied to a problem within a domain, solutions emerge. A single product architecture represents a single solution. However, as we have covered extensively, when attacking problems in the same domain with similar business goals in mind and leveraging similar technology, similarities will emerge in solution architectures. These similarities can be captured in a *reference architecture*. Here, we repeat the definition found in Chapter 3.

**Definition.** *Reference architecture* is the set of principal design decisions that are simultaneously applicable to multiple related systems, typically within an application domain, with explicitly defined points of variation.

As sets of principal design decisions, reference architectures are themselves architectures. However, they are generic or variegated such that they are applicable to multiple systems simultaneously—in the context of the terms we have used in this chapter, to a population or a product line of systems. Points where the architecture can vary from family member to family member are explicitly defined as part of the reference architecture.

There are many different kinds of reference architectures; this definition is intentionally broad. They differ in how they express the commonalities and the points of variation in a population or product line. Three classes of reference architectures include:

**Complete single product architecture:** An ordinary product architecture of a simple toy example or a complete system for a particular domain can be considered a reference architecture, since it might serve as an exemplar for future products in the same domain. Such reference architectures are relatively weak because they do not provide much engineering guidance as to how to use the reference architecture to create new systems.

**Incomplete invariant architecture:** A partial architecture can be specified that is constant and unchanging among all products. Parts of the architecture that vary from product to product are left unspecified, although some design guidance might be provided as to how to “fill in the blanks” in the architecture.

**Invariant architecture with explicit variation:** This kind of reference architecture can be used to simultaneously capture both the invariants *and* the variants in products in a domain.

#### Developing a Reference Architecture

Developing a reference architecture is a serious decision, since it will be the guiding foundation for a number of future products. Determining when, how, and why to develop a reference architecture is critical to success.

##### *When to Develop a Reference Architecture*

An obvious question that arises in DSSE is “when is the right time to develop a reference architecture?” Choosing an appropriate time is critical, since a reference architecture will effectively constrain and bind all solutions in the domain. Premature development of a reference architecture can be disastrous if the architecture is not validated or the stakeholders’ understanding of the domain is too incomplete: instead of just affecting one product, a mistake made in a too-early reference architecture will propagate to many products and vastly increase the costs of that mistake. On the other hand, developing a reference architecture too late can be equally costly: if many diverse solution architectures have already been developed in a domain, then there will be little opportunity to adapt these existing architectures to fit the reference architecture (they will become ‘legacy systems’), and therefore substantially limit reuse benefits.

A good tactic that mitigates some risk is to adopt an incremental approach with respect to reference architecture. The reference architecture should still be developed with the entire family of products in mind—if this is not done, it may take on the characteristics of a single product and have to be significantly adapted later to incorporate the full family. If, as is often the case, a number of products have already been developed and they are being adapted to use a reference architecture, it is usually easier to adapt one or two products at a time to use the reference architecture rather than try to unify the family all at once. Starting with the products whose

existing architecture is closest to the target reference architecture is generally a good idea. This will allow the reference architecture to be evaluated and refined without affecting too many products simultaneously.

#### *Choosing the Form of a Reference Architecture*

Selecting how to capture a reference architecture depends on the domain, the stakeholders, and the underlying business needs of the organization(s) involved. More specific modeling techniques (like the use of explicit variation points) make it easier to detect and prevent phenomena like architectural drift and erosion, but might also limit creative freedom and opportunities for innovation.

As we stated above, a complete single product architecture offers the least guidance to architects as to how to elaborate it into a family of products (unless the products in that family have architectures that are very close to the reference architecture). If this form is chosen for the reference architecture, explicit documentation of the underlying style, what is allowed to change, and what is not should be provided as well. It may also be useful to include several examples of complete product architectures in a family to illustrate this.

Incomplete invariant architectures have the advantage that they tell architects in no uncertain terms what must be present in a family member’s architecture. However, they may lack details about how to actually complete the elaboration process. Again, important documentation about the style and how elaboration should proceed is important. Another (somewhat costlier) alternative is to combine this with complete product architectures: that is, as part of the reference architecture, provide both the incomplete invariant architecture *and* one or more elaborated product architectures (even if these are only samples or demonstration architectures) as these can serve as examples for future elaborations.

Invariant architectures with explicit variation points provide the most direction to architects: not only do they say exactly what must be present in every family member’s architecture, but they also effectively define all the members of the family. A reference architecture in this form may have a large number of variation points, and the combination of all possible combinations of variations will create a number of family members that far exceeds the business needs of the developing organization. For example, imagine such a reference architecture that defines 8 optional features that may be included or not included. This reference architecture defines a family of  $2^8 = 256$  possible architectures. Not all of these architectures will be feasible (due, perhaps, to feature conflicts) or desirable to produce (due to market conditions). These reference architectures make it easy to select family members, but limit the scope of what products can be in the family at all.

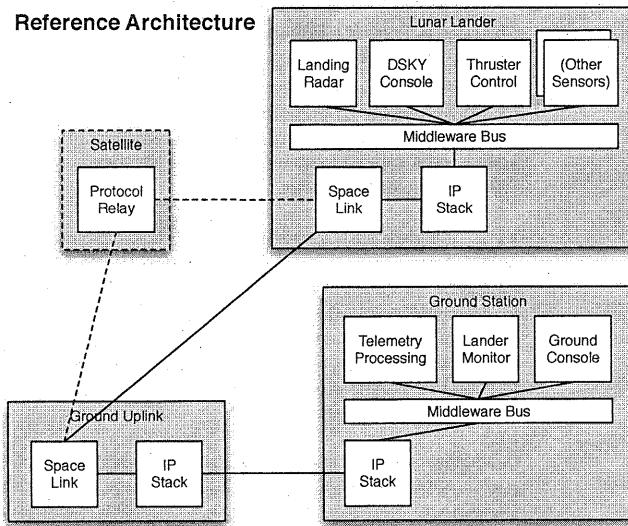


Figure 15-20. Example reference architecture structural view for a Lunar Lander system.

For a complex domain, a reference architecture will be extremely complex and detailed. It would be elaborated with multiple coordinated views as well as extensive documentation capturing the invariants and variation points, as well as guidance on how to refine the reference architecture into a concrete application. Rationale for the various decisions embodied in the architecture would also be included. A structural view such as the one shown in Figure 15-20 might be part of such a reference architecture. This depiction alone is not enough to interpret its intent; supporting documentation is also needed. For example, it may be that the components shown are intended to be the only components in the system, or implementers may be advised to add additional components as necessary. Certain points of variation are obvious: whether or not a relay satellite is used, the type of middleware, the implementation of the space link, the “other sensors” on the Lander, and so on. The intended interpretation of all these elements should be contained in ancillary documentation; this is typical of a reference architecture.

#### 15.2.4 Product Lines and Architecture

There are many significant differences between designing a single product architecture and a reference architecture, chief among them that a

reference architecture must serve as the basis for many different products simultaneously. This introduces a whole host of new issues: not only must the architecture suffice for a single solution, but must be developed, visualized, and evaluated in terms of a large number of potential solutions (many of which may never even be elaborated or developed).

Here is where the technologies and techniques developed in the *product line architecture* community are applicable. Product-line architectures give stakeholders tools with which to diversify an ordinary product architecture into an artifact suitable for describing many similar/related products: a *product line*. The techniques presented here allow stakeholders to develop multi-product architectures without losing the benefits that we have identified in the single-product case: explicit models, visualization, analyzability, and so on.

Product lines are one of the potential ‘silver bullets’ of software architecture—a technique that has the potential to significantly reduce costs and increase software qualities. The power of product lines comes directly through *reuse*, specifically the *reuse* of:

- Engineering knowledge
- Existing product architectures, styles, and patterns
- Pre-existing software components and connectors

Earlier in this chapter, we introduced product lines and product populations. Product lines abound in daily life. We have already discussed consumer electronics and how related products can form a product line (and groups of products can form a product population).

#### 15.2.5 Product-Line Concepts

Here, we will introduce different notions of product lines and how they are developed and defined, as well as elements that go into making up a product line.

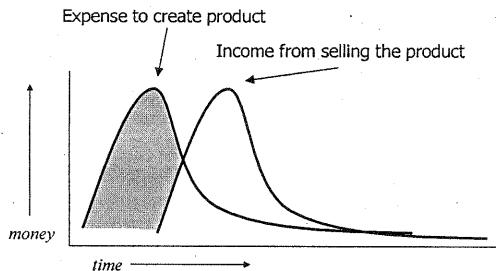
##### Business Product Lines

A business product line is a set of products tied together to achieve a business/monetary purpose, such as increasing sales by bundling products. These products do not necessarily have to have any similarity from an engineering perspective—it is not uncommon for a company who has just acquired new subsidiaries to put all the new products into a single product line to better market the products together.

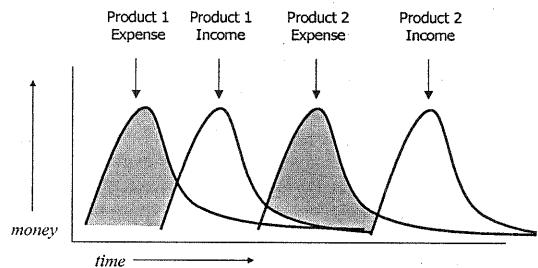
##### Sidebar: Business Goes where Money Flows

In a business based on product sales, there is a gap between expense and income. Money is spent during product creation, but income does not

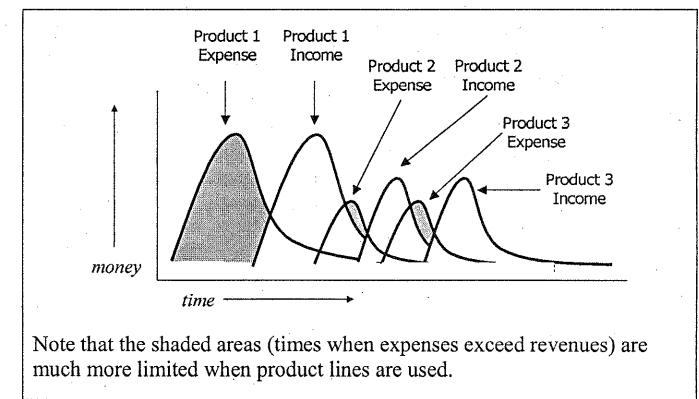
begin to arrive until the product is available in the market. This situation is depicted in the following graph, with the shaded area representing the initial outlay of capital required for product development.



If traditional development practices are used, additional products will have similar timelines:



The use of product lines, however, lowers the development cost and time for making a new product in the product line. In doing so, additional revenue can come in earlier, reducing the effect of expenses that are incurred, like so:



### Engineering Product Lines

Products in an engineering product line are tied together by similarities in how they are designed or constructed. Often, a product line will be both a business and engineering product line, but this is not always the case. For example, from an engineering standpoint the Chrysler Crossfire is nearly identical to a Mercedes SLK V6, but this similarity is not emphasized to consumers, probably due to wide differences in consumer perceptions of these brands. Engineering product lines often share significant portions of their architecture, and the products within them may all conform to a broader DSSA. The product lines discussed in the remainder of this chapter are engineering product lines; however Section 15.2.10 will discuss strategies for unifying disparate products (perhaps those in a business product line) into an engineering product line.

#### 15.2.6 Specifying the Architecture of a Product Line

The architectures of product lines are somewhat different from reference architectures in a DSSA. In general, product-line architectures capture the complete architectures of multiple related products simultaneously. Conversely, reference architectures can be incomplete or partial. They may, for example, specify the architecture of a single product with loose guidance about how to adapt it to other contexts. They may also specify only invariant parts of an architecture and leave the rest up to solution developers.

Product-line architectures differ from reference architectures in two ways. The first difference is one of scope: rather than attempting to describe the architectures of many (potentially diverse) solutions within a domain, product-line architectures focus on a specific, explicit set of related products, often developed by a single organization. The second difference

is one of completeness: product-line architectures generally capture multiple complete product architectures rather than leaving parts undefined.

Recall our characterization of architecture as the set of principal design decisions about a system. A product-line architecture can be similarly defined: a product line architecture captures the principal design decisions of many related products simultaneously. Some of these design decisions will be common among all the products, some will be common among a subset of the products, and some will be unique to individual products.

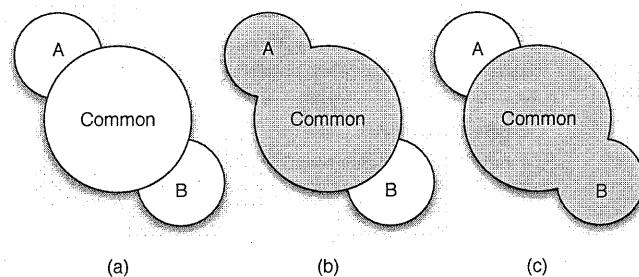


Figure 15-21. A product-line architecture conceptualized as a Venn diagram.

Figure 15-21 shows a product line architecture with two products conceptualized as a Venn diagram. The large center circle represents the design decisions common to all products in the product line. The 'A' shape represents the decisions that are unique to Product A. The 'B' shape represents the decisions that are unique to Product B. Figure 15-21(a) shows the three groups of design decisions. Figure 15-21(b) highlights Product A: the union of the common design decisions and the 'A' design decisions. Figure 15-21(c) shows Product B: the union of the common design decisions and the 'B' design decisions.

To further discuss product-line architectures, we turn again to the Lunar Lander example. Although we have discussed different variations of the Lunar Lander game in earlier chapters, each variation has been discussed in isolation. Product-line architectures give us the power to specify and discuss a family of Lunar Lander games in terms of explicit variations between the family members. The constructs we will introduce to make this possible are *variants* and *versions*.

### Variants

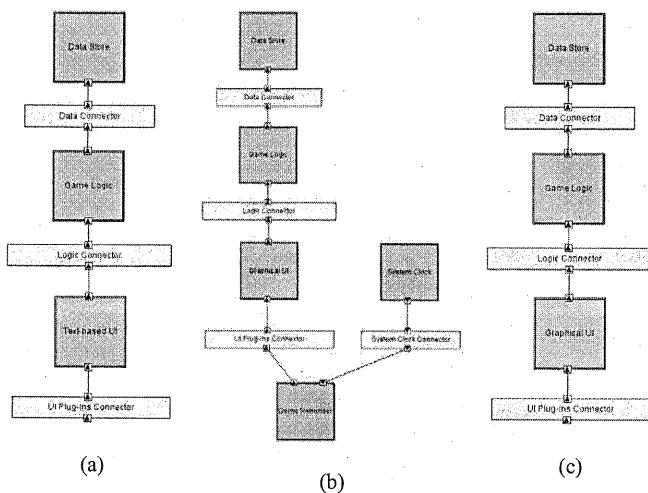
Extending an ordinary software architecture into a product line architecture can be accomplished through the addition of *variation points* to create *variant* architectures. Each variant architecture represents a

different product—a member of the product line. A *variation point* is a set of design decisions that may or may not be included in the architecture of a given product. Variation points identify where the design decisions for a specific product architecture diverge from the design decisions for other products. Each variation point is accompanied by a condition that determines when the design decisions for that variation point are included in a product's architecture. In the above example, the inclusion of the 'A' design decisions can be seen as a variation point. The condition for this variation point is simple: the decisions are only included if the product being built is Product A.

By isolating and codifying variation points, a large number of product architectures can be described compactly by exploiting the different combinations of variation points. Consider a hypothetical product-line of Lunar Lander games. This product line consists of three slightly different Lunar Lander products: Lunar Lander Lite, Lunar Lander Demo, and Lunar Lander Pro.

Lunar Lander Lite is intended as a freely-distributed Lunar Lander game with a text-based user interface. It resembles the Lunar Lander games discussed in earlier chapters, such as those implemented in Chapter 9. Lunar Lander Pro is intended as a commercially-sold Lunar Lander game with a fancier graphical user interface. Internally, the data store and game logic are identical to Lunar Lander Lite's; the only difference is in the user interface component. Lunar Lander Demo is a freely-distributed but time-limited version of Lunar Lander Pro. It has the same graphical user interface as Lunar Lander Pro, but it expires and is not playable 30 days after installation. Periodically, it reminds the user that if they want to continue playing beyond the 30-day limit, they are required to purchase or upgrade to Lunar Lander Pro.

**Figure 15-22.**  
Architectures of Lunar Lander (a) “Lite,” (b)  
“Demo,” and (c) “Pro.”



The architectural structures of all three Lunar Lander products are shown in Figure 15-22<sup>18</sup>. Figure 15-22 (a) shows Lunar Lander Lite, consisting of a data store and game logic component, along with a text-based UI. Figure 15-22 (b) shows Lunar Lander Demo, with a graphical UI component in place of the text-based UI, and an additional demo reminder and system clock that plug into the user interface to remind the user to register. Figure 15-22 (c) shows Lunar Lander Pro, identical to Lunar Lander Demo but missing the Demo Reminder and System Clock components.

**Table 1.** Elements present in each Lunar Lander product-line member.

	Data Store	Data Store Connector	Game Logic	Game Logic Connector	Text-based UI	Text-based UI Connector	Graphical UI	Graphical UI Connector	System Clock	System Clock Connector	Demo Reminder
Lite	X	X	X	X	X	X					
Demo	X	X	X	X	X	X	X	X	X	X	X
Pro	X	X	X	X			X	X			

Table 1 shows the elements—in this case components and connectors—included in each of the three product-line members. This kind of table is good for deciding whether and how to create a product-line. Here, it is obvious that there is significant commonality and overlap between each of the three products—good motivation for creating a product line.

Once the creation of a product-line begins, it is a good idea to group low-level elements into variation points. Recall that each variation point represents a set of design decisions that may or may not be included in the architecture. This allows product-line architects to think about products in terms of features rather than low-level elements. For example, while it is conceivable to think of a product that contains a System Clock Connector but no System Clock, in practice this doesn’t make much sense.

<sup>18</sup> The Lunar Lander example in this chapter will focus on structural design decisions; however, the techniques described apply, in general, to broader kinds of design decisions that go beyond just components and connectors.

Table 2. Grouping architectural elements into variation points.

	Data Store	Data Store Connector	Game Logic	Game Logic Connector	Text-based UI	UI Plug-ins Connector	Graphical UI	System Clock	System Clock Connector	Demo Reminder	
Core Elements	X	X	X	X		X					
Text UI					X						
Graphical UI							X				
Time Limited								X	X	X	

A mapping of elements to variation points is shown in Table 2. Here,

elements common to all products are grouped into “Core Elements.” Three other variation points are defined as well: the inclusion of a textual UI, a graphical UI, and whether or not the product is time-limited. The grouping of architectural elements or design decisions into features is often motivated by domain constraints, business goals, and the individual dependencies and exclusion relationships between the elements.

Ultimately, these groupings must be chosen and defined by system architects—their creation is not an algorithmic process. Variation points will have dependencies and exclusion relationships as well: for example, all variation points depend on the inclusion of the Core Elements, and at least one of the two user interface variation points must be included in a product. These relationships and constraints must be carefully documented.

Once the variation points have been defined, individual products can be specified as combinations of the variation points. For business reasons, or reasons of variation point compatibility, not all combinations of variation points will be made into products.

Table 3. Products as combinations of variation points.

Core Elements	Text UI	Graphical UI	Time Limited
Lunar Lander Lite	X	X	
Lunar Lander Demo	X		X
Lunar Lander Pro	X	X	

Table 3 shows the creation of the three Lunar Lander products from the variation points defined in Table 2. Assuming that the core elements are always included, the three variation points altogether create  $2^3$  or 8 potential products, of which three have been selected for construction. In addition to helping people understand the differences between the different product-line members, this kind of table is often useful in generating ideas for new products using the variation-point combinations *not* selected. For example, one could conceive of a Lunar Lander game that includes both a textual *and* graphical user interface, perhaps giving the user multiple ways of interacting with the game and viewing its state. One could also imagine a time-limited version of the game with a textual UI, or a time-limited version with both user interfaces.

By unifying common features and documenting these explicit variation points, we can combine these three individual architecture descriptions into a single product-line architecture. A few architecture description languages such as Koala [213], discussed later, and xADL [51] allow you to do this directly.

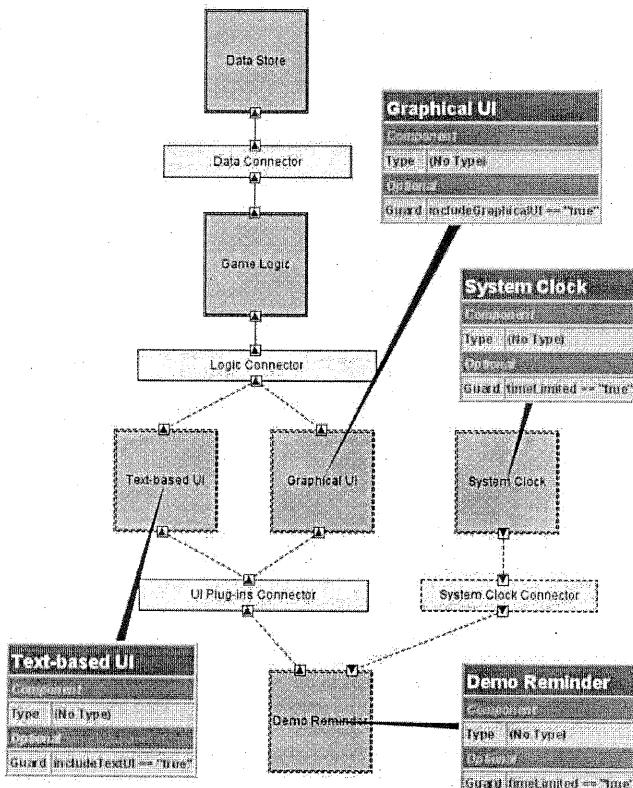


Figure 15-23. Lunar Lander product line architecture.

The combined product-line is shown in Figure 15-23, here in xADL's graphical visualization using xADL's product-line features [54] to express the points of variation. All elements from all products are shown together. Elements such as the Data Store and Game Logic components that are part of the 'core' are represented normally. Elements that are included in one or more variation points are represented as *optional*. Each optional element is accompanied by a guard condition that indicates when it should be included in a product. In this product-line, three variables—`includeTextUI`, `includeGraphicalUI`, and `timeLimited`—correspond to the variation points defined in Table 2. By setting the value of any of these variables to 'true,' the elements corresponding to that variation point will be included in the architecture.

xADL's use of a Boolean expression language to document these guard conditions gives it additional expressive power, including some ability to constrain relationships between features. For example, the Text UI and Graphical UI features could be made mutually exclusive by unifying the `includeTextUI` and `includeGraphicalUI` variables into a single variable, say '`uiType`', whose value would be either 'graphical' or 'textual,' but not both.

### Selection

The process of reducing a product line into a smaller product line or a single product is known as *selection*. Selection involves evaluating the conditions associated with each variation point, and either including or excluding the associated design decisions.

Consider the Lunar Lander product line. By fixing the '`includeTextUI`' variable to 'false,' we have selected only products that do not include a textual UI. This reduces the total number of potential products in the product line from 8 to 4. By also fixing '`includeGraphicalUI`' to 'true,' we can select only those products that include a graphical UI. Now, the total number of potential products is 2. By fixing the final variable, '`timeLimited`,' to 'true,' we can reduce the product line to a single product—one without a textual UI, with a graphical UI, and that is time-limited. This product, incidentally, is the Lunar Lander Demo product—something easily seen by referring to Table 3.

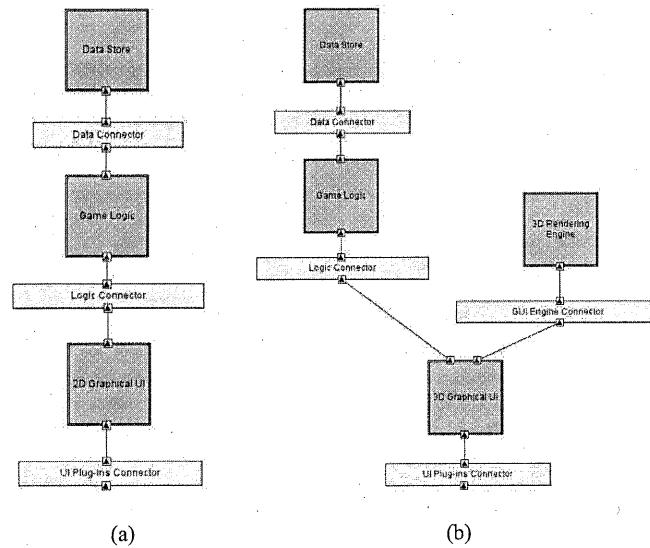
Without tool support, product-line selection must be performed manually—either on the fly in the minds of the stakeholders interpreting architectural models, or by creating and maintaining explicit models of each product in the product-line. Using an approach that supports the explicit specification of variation points and product-lines such as Koala or xADL can make the selection process substantially easier. Specifically, in these approaches product-line selection can be performed automatically through the use of tools. xADL's product-line selector tool allows users to bind values to guard variables, and then reduce a product-line architecture such as the one shown in Figure 15-23 into a single-product architecture such as those shown in Figure 15-22 with a few clicks of the mouse.

### 15.2.7 Capturing Variations over Time

The products in a product line are often alternatives to one another, intended for simultaneous development and release. This is the case with the Lunar Lander product line described above. However, product line architectures can also be used to capture different versions of the same product over time. In general, different versions of the same product will have relatively similar architectures unless something drastic such as a

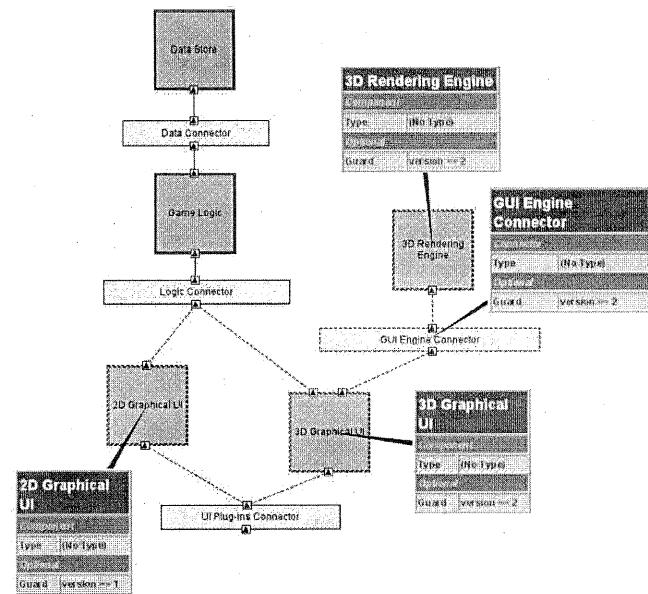
complete redesign or rewrite occurs. When this is the case, it is possible to enumerate the design decisions in both architectures and determine what changed from one version of a product to the next. These can be turned into variation points and encoded into a product line, where the different products are not alternatives, but rather the same product at different times.

Figure 15-24. Two versions of a Lunar Lander game: version 1 (a), and version 2 (b).



Consider an evolving Lunar Lander game. The first version of the game might include a graphical user interface with two-dimensional graphics. A second version of the same game, released later, might differ by including a graphical user interface with three-dimensional graphics, supported by an off-the-shelf 3D rendering engine. These two product architectures are shown in Figure 15-24 (a) and (b), respectively.

Figure 15-25. Product line of Lunar Lander games where each product is a version of Lunar Lander.



Clearly, this situation mirrors the situation seen earlier when the products were different games to be marketed, rather than versions of the same game. Using the same mechanisms described above, the two versions of the game might be encoded into a single product line, with each product representing one version of the game. This product line is shown in Figure 15-25. Here, the version is selected using a single variable, ‘version,’ rather than by choosing a combination of variation points.

### 15.2.8 Using Product Lines as Tools for What-If Analysis

Above, we have discussed how product lines can be used to capture variations across related products and across different versions of the same product. Another application of product lines is to capture design alternatives. Design is often an exploratory process—it involves making decisions and tradeoffs that will affect the properties and construction of the target products. Questions arise: should we include this component or that component? Should this part of the application run on the client or on the server? Oftentimes, it will be unclear what the best path is, so multiple alternatives are considered and pursued for a period of time until more information becomes available.

When this happens, product-line techniques can be used to simultaneously capture alternative architectures. Here, each product is not a system that is intended to be built, but one of many potential product designs. Points of variation in these product lines are decision points. The selection process can be used as a form of ‘what-if’ analysis.

Software engineers have had to deal with variations, evolving artifacts, forking, branching, merging, and related concepts for years, particularly in the area of source code. In general, they are assisted in these regards by software configuration management systems. Configuration management systems can also be used to help address these concerns when dealing with artifacts such as architectural models, especially when the artifacts themselves offer no explicit support for these concepts.

One simple approach is simply to put architecture models into a version control system such as RCS [283], CVS [79], Subversion [44], or ClearCase [12]. This is a viable option for versioning architectures as a whole, and it helps track the evolution of architectures over time. To some extent, alternatives can be created through branching revisions.

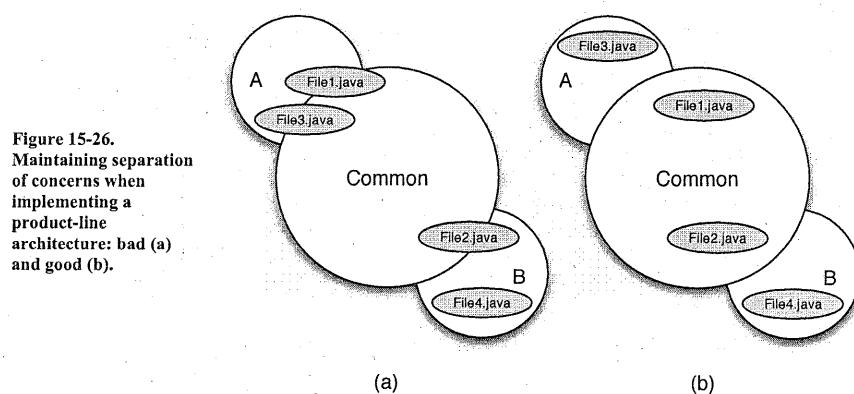
This approach does not work particularly well for creating or maintaining product-line architectures. Managing a product-line architecture means establishing a core set of design decisions and then combining those core decisions with variation points consisting of additional decisions. In general, design decisions are spread throughout and across architectural models, and this is why architecture description languages like Koala and xADL embed the variation points within models. Because version control systems generally work at the level of files, it is difficult to use them to manage elements within files—for example, a component specified inside an architectural model.

A compromise is to attempt to separate out core parts of architectures and variation points into separate files, and then manage the evolution of these elements independently in a version control system. This works in theory, but in reality it is difficult and inconvenient to have related design decisions for a single product-line member scattered across files, especially when automated merging tools are not available to merge them together again.

#### Sidebar: Configuration Management of Architectures

architecture. Here, flexibility in connectors and communication methods is a primary driver of product-line reuse. If an architecture is chosen where components and connectors are tightly bound, it will be extremely difficult to introduce points of variation without recoding existing components. However, if flexible connectors and communication styles (such as message passing) are used instead, it is possible to more easily introduce variations in the architecture without making extensive changes to existing components. However, having flexibility at the architectural level does not necessarily mean that the same flexibility will be present at the implementation level.

Chapter 9 discussed how implementing a system built using software architecture techniques is largely a mapping problem: understanding and controlling how design decisions made in the architecture map to implementation artifacts. In general, all the advice in Chapter 9 applies here as well. Implementing a product-line architecture is still a mapping problem, except that multiple products composed of core elements and variation points are involved. In this case, separating concerns in the implementation artifacts along the boundaries of variation points in the product line is critical.



**Figure 15-26.**  
Maintaining separation  
of concerns when  
implementing a  
product-line  
architecture: bad (a)  
and good (b).

Consider the situation presented in Figure 15-28. In Figure 15-28 (a), good separation of concerns has not been maintained in the implementation. Various source files (File1.java, File2.java, and File3.java) are responsible for implementing both core concerns as well as product-specific concerns. In this case, neither Product A nor Product B can be constructed without importing at least part of the implementation of the other. This makes it hard to evolve the products independently, and to integrate new products into the product line. Figure 15-28 (b) shows a good separation of

#### 15.2.9 Implementing Product Lines

The major reductions in implementation costs from using a product line come about primarily through extensive reuse: where two products in a product line share a similar architecture, the implementations should be (virtually) identical. Achieving this level of reuse must start in the

concerns: here, implementation artifacts corresponding to products are kept separate from the common core and from each other. Both products can be built without the need for artifacts that (partially) implement other products.

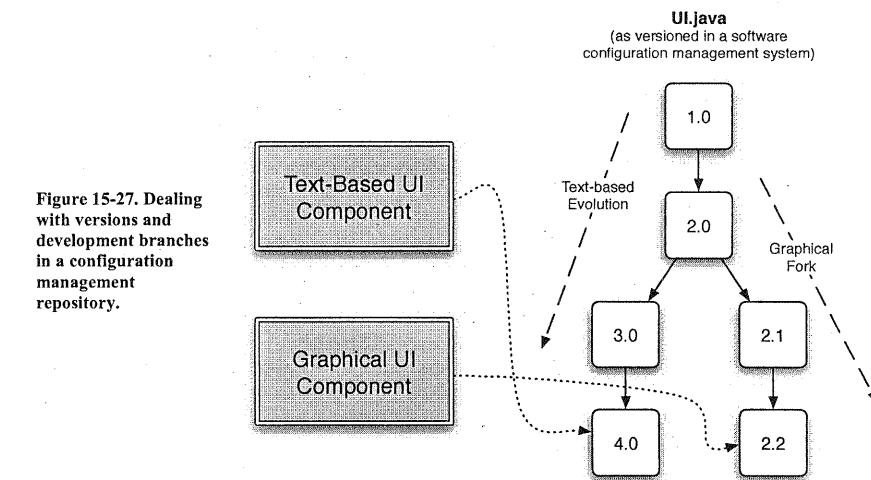
One way of maintaining this separation of concerns is to use flexible architecture implementation frameworks, as discussed in Chapter 9. Many implementation frameworks help to enforce loose coupling between component and connector implementations, such that components and connectors can have their dependencies changed easily and automatically. Implementation frameworks often allow components and connectors to be bound to each other “late”—either at product build-time or even dynamically at run-time. Implementations that employ late bindings of components generally enforce better separation and independence of components and help to drive reuse. Interface-implementation separation is also important: well-defined implementation-level interfaces help to establish what services are provided (and required) by a component (or set of components) without requiring a particular implementation. This separation of concerns further increases flexibility: changes to the implementation of one component will not require changes to other components if the contract of the interface is maintained.

This is not always easy to achieve, however: oftentimes, legacy products are incorporated into a product line. These products may not use flexible components, connectors, and communication methods. In this case, a careful refactoring should be considered, driven by the product-line architecture. Tight bindings in a product line are workable as long as they do not interfere with or cross the points of variation. For example, if three core components that are part of every product in the product line are tightly coupled, this is not a major problem: these components will never be separated, so making their bindings to each other flexible will be of limited near-term value. Instead, developers and architects should focus on making the bindings to components that exist only in a few products more flexible.

#### Product Lines and Source Code Management Systems

Any mature development project will leverage some form of configuration management tool-set to keep track of different versions of lower-level implementation artifacts: code files, resource files, and so on. Successfully managing product line implementations requires an understanding of the relationship between versions of architecture-level elements (components, connectors) with versions of implementation-level elements (code, resource files) as stored in a configuration management repository. If implementations are cleanly separated along the lines of architectural elements, this simplifies the mapping problem greatly.

One phenomenon that occurs more often in product-line development than in single-product development is the use of multiple versions of the same implementation artifact (e.g., source file) in different places in the product line architecture. For example, recall the Lunar Lander product line shown in Figure 15-23. Perhaps, for whatever reason, the implementation of the text-based user interface and the graphical user interface were based on the same code, a single file called “UI.java,” that has evolved over time. At some point in the past, a fork of UI.java was created in the configuration management repository, without renaming the file. Thus, there are two development branches of UI.java: one for a textual UI and one for a graphical UI.



**Figure 15-27.** Dealing with versions and development branches in a configuration management repository.

This situation is depicted in Figure 15-28. Here, the Text-based UI component uses version 4.0 of `UI.java`, while the Graphical UI component uses version 2.2. In a situation like this, implementation mappings must not only refer to individual files, but also individual *versions* of individual files to capture the appropriate level of detail.

#### 15.2.10 Unifying Product Architectures with Different Intellectual Heritage

Unfortunately, product lines are not always considered at the inception of a group of related products. The idea of using product lines often appears on an organization’s “radar” only after it has developed many products that have similar functionality and has duplicated an enormous amount of effort in doing so. Alternatively, company mergers and acquisitions can

leave a single organization with the responsibility for developing, maintaining, and evolving very similar (and at one time, competing) products. At this time, the use of product lines becomes extremely attractive as a way of cutting costs by reusing engineering knowledge and architectural decisions from one product to the next. The difficulty is that the existing products in the product line often share little intellectual heritage, and the product architectures differ widely.

This is one of the most difficult problems in product-line development. The primary tension is that the goal of using a product line is to enable reuse, but the existing products exhibit little to no reuse.

When this is the case, attempting to develop a product-line architecture that includes all the existing products may be of limited value, except as a historical artifact. Instead, processes should be forward-looking: attempting to extract the architectural lessons of previous projects and unifying them into a product line for future products (or future product versions).

Before a product-line architecture can be developed, individual product architectures must be obtained. Architecturally-savvy organizations will probably have documented architectures for their products already, but as we have discussed many product architectures evolve organically or diverge from their original intentions. In this case, architectural recovery (discussed in Chapters 3 and 4) is the first step toward product-line development.

The next step of the process is to normalize the existing product architectures (if necessary). Often, even when architectures for each product are available, they may not capture the same aspects of the systems under development, or capture those aspects at the same level of detail. They may not use the same terminology to refer to similar concepts. When this is the case (and it nearly always is) some amount of normalization must occur—some of the architectures must be elaborated so that the commonalities and differences among the product architectures can be more readily identified. Luckily, architecture elaboration in this situation is made easier by the fact that there are actual, implemented products from which to extract the additional information needed.

When normalized product architectures are available, they can be compared to identify common aspects and points of variation. Unless all the architectures are expressed in the same notation at the same level of detail, it is probably not possible to automate much of this process. Instead, it is more useful to gather the architects and other stakeholders from each product into a series of meetings. Developing tables similar to

Table 1 and Table 2 in order to understand the overlap between features and elements in the various products may be a useful exercise.

Developing a product-line architecture from this point forward is then a stakeholder-centric activity. There is no “one right way” to go about this, and depending on the domain and the organizational goals, the effort may go in one of many different directions:

- **No Product Line:** It may be determined that, after examining the architectures, less reuse is possible than previously imagined. Perhaps the products were thought to perform many similar functions, but in reality they serve different purposes. Alternatively, the products may be so architecturally different that attempting to unify future versions of the products into a product line would cost more than the potential reuse would save. Here, the best alternative might be to abandon the idea of developing a product line entirely, and focus on further distinguishing the products from one another in separate development efforts.
- **One Master Product:** Often, the easiest course of action in developing a new product line is to identify the best existing product and use its architecture as a basis for a product line. In this way at least one product will fit naturally into the emergent product line, and innovative features from other products can be integrated as appropriate.
- **Hybrid:** When no one product can be identified as the master for the purpose of developing a product line, the ‘best of breed’ features of each product in the domain can be extracted and unified into a hybrid product line. Here, no one existing product will fit totally naturally into the product line architecture. This is most useful when new products are not intended to be direct descendants of old products, or when existing products are being unified.

### 15.2.11 Organizational Issues in Creating and Managing Product Lines

This chapter has largely covered the creation and management of product lines and product line architectures from a technical perspective. However, using product lines is not a solely technical activity. As is indicated in the business case sidebar at the end of this chapter, a product-line-based approach needs to be as much organizational and cultural as it is technical. Creating a product line often means integrating the needs and opinions of stakeholders from fundamentally different product teams into the same effort. This can foster all kinds of organizational and technical issues: friction between the teams, feature creep, least common denominator architectures, and so on.

Furthermore, an organization's investment strategy in its products needs to change to match a product-line approach. Creating a product line incurs substantial costs that do eventually pay off, but not in the context of a single product. Rather, they are recovered through lower maintenance expenses across multiple products and the increased profits from selling more product variants. This requires organizations to think *horizontally*, across product and team boundaries, which often requires both an organizational and cultural shift.

Clements and Northrop have written extensively about these issues in their book *Software Product Lines: Practices and Patterns* [41], and we encourage interested readers to look to this and other sources for more detailed guidance in this regard.

### 15.3 DSSAs, Product Lines, and Architectural Styles

Throughout the chapter, we have discussed both domain-specific software architectures (DSSAs) and product lines, as well as their relationship to each other. A natural question arises at this point: what is the relationship between DSSAs, product lines, and architectural styles?

Recall that architectural styles represent a reusable 'package' of design decisions that can be applied to different products to elicit desired qualities. In some sense, both DSSAs and product line architectures can be seen in the same light. Usually however, architectural styles are far more general than DSSAs or product-lines. Most architectural styles can be applied across many domains. For example, the pipe-and-filter style has been used to develop text processing applications, typesetting systems, and program compilers. Typically, such diverse applications would not all be members of the same DSSA or product-line.

Styles do, however, play an important role in the development of both DSSAs and product lines. It would be unusual for different products in the same DSSA or product line to have significantly different architectural styles. As noted above, one of the canonical requirements that is often identified in the development of a DSSA is the architectural style that will be used to create applications within the DSSA. Typically, a reference architecture for a DSSA will follow this prescribed style. Similarly, individual products in the same product-line architecture will generally follow the same style. The use of a common style across a DSSA or product-line is ultimately an effort to ensure consistent qualities in the products that emerge, and keep them from drifting away from the original intent of the product-line.

Just as there can be points of variation in architectures, there can also be points of variation in architectural styles themselves: different sets of constraints to solve related problems. By applying product-line

architecture techniques to the decisions that compose architectural styles rather than architectures, it is possible to create a family of architectural styles.

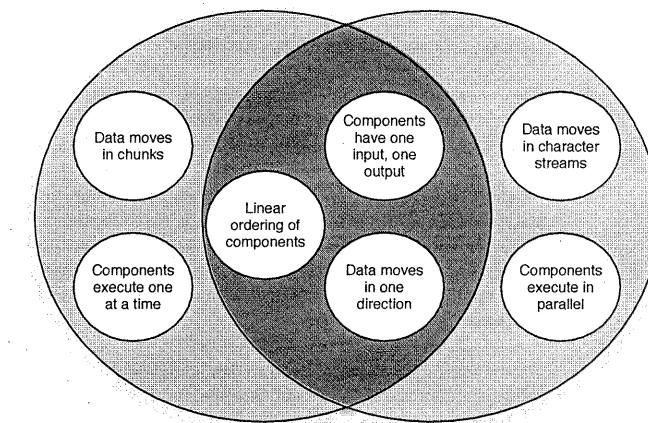


Figure 15-28. An example of related architectural styles.

Recall two of the most basic architectural styles from Chapter 4: batch-sequential and pipe-and-filter, as shown in Figure 15-28. These styles actually share many constraints in common: for example, both enforce a linear ordering of components, each of which has one input and one output, and data moves unidirectionally through the line, being processed individually by each component. They differ in a few details: batch-sequential systems pass the data wholesale in a chunk, and only one component operates on the data at a time; pipe-and-filter systems pass data as it is available and components execute in parallel when possible. Here, explicit variation points can be used to express and reason about the relationship between architectural styles just as they are used to reason about the relationship among software products.

### 15.4 DSSE Examples

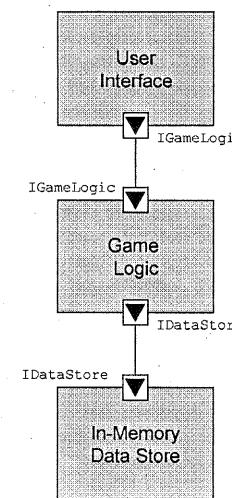
In this section, we present two examples of how domain-specific software engineering techniques, including product-line architectures, have been applied in software development practice. The first example is Philips Electronics' use of the Koala architecture description language in the development of software for devices in the consumer electronics domain. The second example is the domain of software-defined radios, configurable devices that communicate using radio waves, with their internal functionality implemented by software.

### 15.4.1 Koala and Consumer Electronics

Consumer electronics is a dynamic and highly competitive domain of product development. For decades, devices such as televisions and cable descramblers were relatively simple devices with a few, well-defined capabilities. Over the years, these devices have become more and more complex, largely due to enhancements in their embedded software. The latest incarnations of these devices include features such as graphical, menu-driven configuration, on-screen programming guides, video-on-demand, and digital video recording and playback. In a global marketplace, each of these devices must be deployed in multiple regions around the world, specifically configured for the languages and broadcast standards used in those regions.

The increasing feature counts of consumer electronic devices are accompanied by fierce competition among organizations, and it is just as important to keep costs down as it is to deploy the widest range of features. From a software perspective, keeping costs down can be done in two primary ways: limiting the cost of software development and limiting the resources used by the developed software (and thus the costs of hardware needed to support it). Additionally, manufacturers often “multi-source” certain parts. That is, they obtain and use similar parts (chips, boards, tuners, etc.) from multiple vendors, buying from vendors who can offer the part at the right time or the lowest price, and providing a measure of insurance against the failure of one particular part vendor to deliver. If the parts are not 100% interchangeable, software can be used to mask the differences.

Product line architectures provide an attractive way to deal with the diversity of devices and configurations found in the consumer electronics domain. Philips Electronics has developed an approach called Koala [213] to help them specify and manage their consumer electronics products. Koala is primarily an architecture description language (derived from the Darwin ADL). Koala also contains aspects of an architectural style, however, since it prescribes specific patterns and semantics that are applied to the constructs described in the Koala ADL. Koala, like Darwin, is effectively a structural notation: it retains the Darwin concepts of components, interfaces (both provided and required), hierarchical compositions (components with their own internal structures) and links to connect the interfaces. In addition to these basic constructs, Koala has special constructs for supporting product-line variability. Koala is also tightly bound to implementations of embedded components: certain aspects of Koala (such as the method by which it connects required and provided interfaces in code) are specifically designed with implementation strategies (e.g., static binding through C macros) in mind.



A basic Koala diagram with no product line variability for a Lunar Lander application is shown in Figure 15-29. As you can see, basic Koala diagrams are effectively equivalent to Darwin diagrams. Koala extends Darwin in the following ways:

**IDL-based interface types:** An interface type in Koala is a named set of function signatures, similar to those you would find in C. For example, the interface to the Lunar Lander data store in Koala might be declared like this:

```

interface IDataStore{
    void setAltitude(int altitudeInMeters);
    int getAltitude();
    void setBurnRate(int newBurnRate);
    int getBurnRate();
    ...
}
  
```

The IDataStore interface type may be provided (or required) by any number of Koala components. When a provided and required interface are connected, the provided interface type must provide at least the functions required by the required interface type.

**Diversity interfaces:** One of the philosophies of Koala is that configuration parameters for a component should not be stored in the component; instead, configuration parameters should be accessed by the

component from an external source when needed. This allows the application to be configured centrally, from a single component (or set of components) whose purpose is to provide configuration data for the application. “Diversity interfaces” are special required interfaces that are attached to components and are used by the component to get configuration parameters.

**Switches:** A switch is a new architectural construct that represents a variation point. It allows a required interface to be connected to multiple different provided interfaces. When the variation point is resolved, only one of the connections will actually be present. Which provided-required interface pair is connected depends on a configuration condition, analogous to the guards we have discussed earlier in this chapter. A switch is connected to a diversity interface to get its configuration parameters, just as a component would. Depending on the values returned through the diversity interface, the switch will route calls to one of the required interfaces connected to it. If this means that there will be disconnected components (i.e., that will never be invoked) then these components will not be instantiated to save resources.

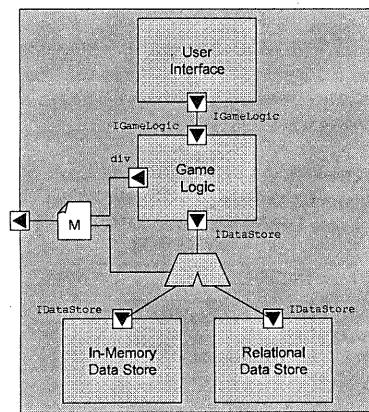


Figure 1  
diagram  
Lander 1  
point.

Figure 15-30 shows a Lunar Lander architecture in Koala with a variation point. Here, the application can use an in-memory data store or a relational data store to maintain application state. The required interface of the Game Logic component is now routed through a switch, which is configured by configuration parameters provided externally. The Game Logic component includes a new diversity interface ‘div’ that allows it to access those external configuration parameters.

**Optional Required Interfaces:** Several components may provide similar, but not identical, services. For example, a basic TV tuner component may have only the ability to change frequencies, but an advanced TV tuner may be able to search for valid frequencies as well. It is possible for callers to a TV tuner to include an optional required interface, and query whether this interface is actually connected or not. If it is connected, the caller can make calls on the optional interface; if not, the caller should behave/degrade gracefully.

Through these mechanisms, Koala gives architects the power to specify and implement product lines of embedded systems. Koala’s main strengths are its straightforward notation, intuitive graphical visualization, and tool support for implementing product lines efficiently. Although developed for the consumer electronics domain, Koala is generic enough for use in many domains.

A drawback of Koala is its lack of support for explicit software connectors (a trait it inherits from Darwin). Koala implies that communication among components happens exclusively through synchronous request-response procedure calls. There is no explicit support for asynchronous or message-passing interaction (message passing, in particular, is a well-known alternative to supporting flexibility and diversity).

Using an architecture-centric approach gave Philips the ability to break their software systems into reusable components that communicate through explicit interfaces, while still retaining the small size and efficiency necessary for embedded systems development. Taking inspiration from an existing architecture description language (Darwin), they defined a domain-specific ADL (Koala) with semantics that mapped well to their application domain and library of components. Additionally, they incorporated explicit support for variability into Koala. This gave them the ability to deal with the many market-induced variations in their product lines (to deal with multiple grades of products with different feature combinations, different requirements due to internationalization, and so on). Rather than maintaining separate architectural descriptions for each product, entire product lines can be captured in a single model. More than 100 engineers at Philips have used Koala, making it one of the most successful industrial applications of ADLs and domain-specific architecture-centric development.

#### 15.4.2 Software Defined Radios

Communication over-the-air has been used to facilitate all kinds of social advances, from early audio and morse-code transmissions to video transmissions for television, to the latest advances in cellular phones and broadband WiFi connections. Traditionally, radio hardware has been

specialized for a particular kind of application: for example, an ordinary car stereo is limited to receiving analog AM/FM audio transmissions: it cannot, for example, decode TV signals (even the audio portion) or act as an Internet WiFi repeater. To do so would require hardware components to be changed out or adapted.

The increased capabilities of digital signal processing components as well as advances in reconfigurable hardware (FPGAs<sup>19</sup> in particular) have made it possible to rethink how communication-over-radio devices are built from both a hardware and software perspective. The result has been an effort to develop so-called ‘software defined radios’ (SDRs) [63]. A software defined radio is a device that can transmit, receive, and process signals over the air for a variety of applications, where the application is defined by the software that is loaded on the radio. Standard components of a software defined radio include an antenna, analog-to-digital conversion, FPGAs for high-frequency digital signal processing, and general purpose processors (such as PowerPCs) for further signal processing duties, as well as various I/O ports for interfacing with audio and video devices (displays, microphones, speakers, and so on).

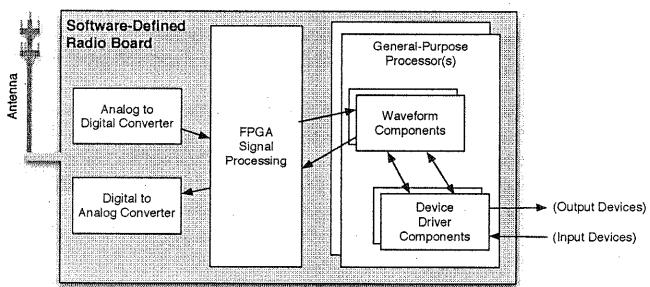


Figure 15-31. Basic data pipeline of a software-defined radio.

The basic data flow through a software-defined radio board is shown in Figure 15-31. Depending on the configuration of the FPGA(s) and the components and connectors loaded on the general purpose processors, the

<sup>19</sup> FPGA stands for Field Programmable Gate Array. An FPGA is effectively an integrated circuit consisting of an array of logic gates that can be reconfigured through software. Once reconfigured, the circuit can perform any function it is programmed for—processing data, cracking encryption, emulating another microprocessor’s instruction set, and so on. In general, FPGAs are not quite as fast as dedicated, special purpose hardware but the performance is reasonably close.

radio can be used for all sorts of applications. In theory, a software-defined radio could act as everything from an ordinary FM radio to a television set to a wireless access point simply by loading different software onto the radio.

The domain of software-defined radios is ideal for the application of DSSE principles. A domain-specific software architecture has been developed for software-defined radios called the Software Communications Architecture [195]. It is described in the sidebar titled “The Software Communications Architecture (SCA).” This particular DSSA is not a panacea, however, and the sidebar touches on many issues that may make it less than ideal.

The organizations interested in developing software-defined radios are keenly interested in the design, particularly the software design, of such radios. This resulted in the development of a standard known as the Software Communications Architecture (SCA), which governs the design of SDRs (although, as the name implies, it is intended for future application to other kinds of communications systems).

The SCA is an interesting document to study, since it is the standard ‘architecture’ that organizations implementing SDRs are intended to follow.

The SCA looks at the software architecture of a software-defined radio as a set of interacting software components. These components are defined and interact via CORBA (see Chapter 4). As one might expect, the choice of CORBA as the sole software interconnection technique induces several architectural consequences on SCA systems, among them:

- The style of an SCA-based software-defined radio is a distributed objects style;
- Interfaces are a primary driver of interaction;
- Provided interfaces for various kinds of components are defined using CORBA IDL;
- Components communicate primarily through synchronous procedure calls to provided interfaces.

The bulk of the SCA specification is a collection of CORBA IDL interface definitions for various kinds of components. For example, filesystem components implement an interface very similar to the POSIX filesystem interface. Other interface definitions exist for different kinds of drivers and other service components.

Actual signal data in the architecture is broken up into digital data packets.

Packets of data are passed from one component to another through a *de facto* call named PushPacket. A component wishing to send a packet of data to another component will call PushPacket and pass the data packet to the target component. Chains of these components create processing pipelines and data flows.

The SCA raises a number of important questions based on what is specified, and what isn't. For example, the architectural style embodied by the SCA is a distributed objects style, with a library of different kinds of components (objects) that can be used to construct SDRs.

It is unclear which came first: the style or the choice of middleware. Ideally, the SCA developers decided that a distributed objects style was the right style for constructing software-defined radios and then chose CORBA as a middleware platform or framework for implementation. However, it is also possible that the SCA developers, encountering heterogeneous hardware platforms and component implementations (especially legacy component implementations embedded in non-software-defined radios), chose CORBA for its services in masking these differences, and the distributed objects style was just fallout from this decision. For the low-bandwidth control pathways in the architecture, distributed objects makes sense, but distributed objects is not a style that comes to mind for dealing with high-throughput data flows of packets passing through a radio. In this case, a hybrid style that had explicit support for streams, or at least asynchronous message-based data flows, might have been more appropriate.

Another question to ask is why CORBA itself was specified in the SCA, as opposed to other middleware that supports a distributed objects style such as COM, or an architecture framework that can be implemented with different kinds of middleware. The intent was likely to support interoperability among independently-developed components, since CORBA is not tied to one particular vendor—many CORBA implementations exist. However, interoperability between CORBA implementations is rarely perfect, and components developed against one implementation may have difficulty working in the context of another. It could be argued that the calling out of CORBA as a core aspect of SCA-based systems is a case of overspecification in the architecture.

The above descriptions talk about which aspects of a software-defined radio are specified by the SCA. It is more important, however, to understand which aspects *are not* specified. The SCA surprisingly provides almost no guidance as to how to develop a radio based on the components and interfaces it defines. It contains little information about how to configure the components, to structure the radio application as a

whole, or how to implement them. This leaves perhaps the most important and difficult decisions about constructing a radio entirely up to the radio developers themselves.

A final question to ask concerns what kinds of software qualities are enabled by the use of the SCA. Portability, composability, and ease of integration are arguably enabled by this architecture, because of the detailed interface specifications and the identification of specific middleware to connect elements. However, are these qualities the most important qualities in the development of a software-defined radio? Arguably, more important qualities like performance and reliability are largely ignored by the SCA, and this is perhaps its biggest problem. At this time, the jury is still out on the success of the SCA; several commercial and military efforts are underway to implement SCA-based radios. However, open-source and hobbyist groups are also implementing software-defined radios using their own architectures and frameworks, and meeting with a measure of success also. Time will tell whether the SCA will bear fruit or not.

The software-defined radio domain is also an example of where product lines can make a significant impact because the domain encompasses so much variability. Variability exists at many different levels of abstraction:

**Network Topology:** In this domain, radio devices do not stand alone: they communicate (via radio links) with other radios running other applications. Although software-defined radios can remain in one location, it is often the case that the radios themselves are mobile—mounted to vehicles or carried by individuals who move around. As such, the topology of devices can change as they move around, or devices go on or offline.

**Radio Configuration:** A single software-defined radio board comprises a channel: a device that can be configured for one particular application at a time. In general, these devices are configured on a single board. More complicated radios support multiple channels by having multiple hardware boards mounted in the same radio backplane. Two-to-eight channel radios are not uncommon for commercial or military applications.

**Board Configuration:** Each board in a software-defined radio can be implemented in a number of different ways. Although the basic elements (antenna, analog-to-digital conversion, and signal processing) are basically the same, they can be configured in different ways. Boards may include different FPGAs, different general-purpose processor

configurations, different I/O ports and controllers, or different amounts of memory or storage.

**Software Configuration:** Each board generally has a number of processing elements on it that can be loaded with software: FPGAs and general-purpose processors, for example. Depending on the application, different components will be loaded onto the different processing elements. Depending on the application, different configurations and topologies of components and connectors will be deployed on the processing elements.

Variability at each of these levels must be understood, controlled, and managed. The first thing to note is that these levels of abstraction are more or less hierarchical: vehicles contain radios, radios contain boards, boards contain processing elements, and processing elements contain software elements. Modeling notations that directly support hierarchical architectures, such as Darwin, Koala, or xADL 2.0, are all good candidates for modeling such an architecture. Variability at each level is also somewhat limited: specific software defined radios will be developed for specific purposes (military, commercial, and so on). Thus, network topologies will have certain common characteristics. For a given organization, only a few different radio and board configurations will be produced: an organization may produce only a 2-channel and a 4-channel radio, for example. Board configurations may be limited to a ‘test board’ and a ‘production board.’ Software configurations will be partially driven by board configuration: each device or controller on the board will likely have an associated device driver component; other components will be driven by the various applications loaded on the radio.

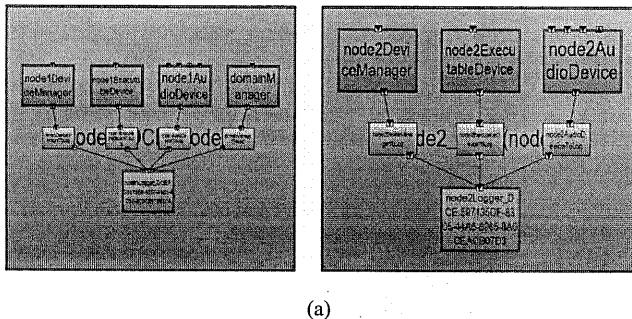


Figure 15-32. Software-defined radio structure with just drivers and operating environment loaded (a), and with a waveform application deployed (b).

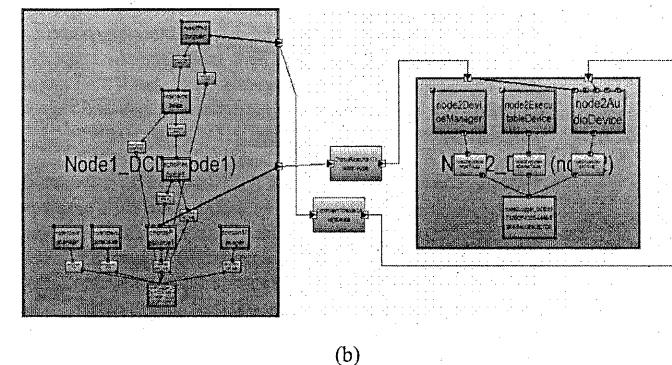


Figure 15-32 shows two different variants of the architecture of a software-defined radio called the SCA Reference Implementation (SCARI), modeled in xADL and depicted in xADL’s graphical visualization. SCARI is a simple example of an SCA-based software-defined radio, intended to demonstrate how the SCA can be used to implement an SDR. Figure 15-32 (a) shows the radio with only the device drivers and operating environment deployed. Figure 15-32 (b) shows the same radio with an additional waveform application deployed. Each represents a different product-line variant, and by assigning guards to each the waveform components using techniques shown earlier in this chapter, waveforms deployments can be selectively applied to the radio using product-line selection.

The extreme flexibility in the domain is induced by increasingly adaptable hardware, but is primarily enabled by software. Since software is so malleable, this should come as no surprise. Because of this, as well as other constraints that must be considered when dealing with SDRs—size, power consumption, performance, time to load and unload waveforms, and so on—SDRs are yet another domain where the capture and reuse of specialized engineering knowledge and experience can substantially reduce costs and risks in the development of new systems.

## 15.5 End Matter

Domain-specific software engineering is, in many ways, the culmination of all the advice given in this book. It broadens the challenge of architecture-based development substantially: instead of just applying architecture-centric principles to a single product, organizations and even entire communities must apply them across a range of related products. This is complicated by the fact that the products already developed in the

domain were developed for different, often competing business goals, by isolated development groups that did not share engineering knowledge or architectural assets in the past. This is perhaps the biggest challenge in architecture-centric software development, but it also has the greatest potential reward: a substantial reduction in costs and risks to develop new systems within an entire domain.

In some ways, the creation of a domain-specific software architecture resembles the development of an architecture for a single product—it still involves the modeling, visualizing, analyzing, and applying principal design decisions. However, it is made even more difficult by the fact that the architecture must serve for a wide range of systems. A constant tension exists between overspecification and underspecification—specifying too much and constraining the kinds of systems you can construct vs. specifying too little and providing insufficient guidance and value. Key contributors may come from different backgrounds and organizations, and may have fundamentally different ideas about how the architecture should be constructed. This chapter has provided a survey of the kinds of artifacts that make up a domain-specific software architecture, and provided some advice about how to create them. However, in the end it is still a very human-centric process of negotiation and cooperation.

Product-line architecture techniques provide a more concrete way to apply domain-specific software engineering “in the small.” Product lines typically are developed within a single organization and target a much narrower set of products. Because of this narrower focus, product-line architectures are often far easier to develop and maintain than DSSEs, since there is far less variation in business goals and there are fewer organizational boundaries to cross. Substantial cost reduction and risk mitigation can still be achieved within the product line, especially if automated tools can help with activities like product-line selection.

The primary attraction, and benefit, of domain-specific software engineering is found through *reuse*. Reuse and continual learning and refinement of knowledge about how to build systems is the hallmark of any engineering discipline. Software reuse has therefore been widely recognized and often touted as a way of controlling the complexity of software systems, improving their reliability, speeding up their development, reducing their associated costs, and so on. However, a cursory look at the practice of software reuse indicates that most frequently it entails *scavenging* source files for needed code fragments, *cloning* modules needed in multiple places in a system (which is, incidentally, something that good software engineering practice discourages), or *purchasing* entire commercial-off-the-shelf (COTS)

#### Sidebar: The Business Case

solutions.

Therefore, reuse in software development is predominantly focused on source code. However, this is misaligned with the near-universal awareness that the key software engineering costs lie elsewhere—in requirements elicitation and system design—and that software architecture is a system’s (and, often, a development organization’s) principal asset. In other words, source code-level reuse is not the most effective way of approaching reuse.

DSSE recognizes and address this discrepancy. It provides mechanisms for expanding the notion of reuse to include all concerns in the development of a software system (so long as that system falls within a particular application domain). This includes:

- the canonical, *reference* system requirements that are in some significant way shared across all systems in the domain,
- the terminology specific to a domain, and sometimes *invented* for the sole purpose of enabling effective software development in that domain,
- the canonical, *reference* architecture, with clearly identified variation points,
- the canonical, low-level system designs that realize the architecture,
- the analysis, simulation, and testing models and tools,
- the domain-specific implementation techniques, off-the-shelf components, and code generators,
- the system construction and deployment scripts,
- the predicted evolution patterns and associated mechanisms,
- the required knowledge and training of software engineers, and
- the processes for managing different projects with shared characteristics, existing domain-specific assets, already developed systems, and systems currently under development, as well as planning future systems.

The argument here is that in theory, this could be done for any software system. In practice, it is not possible. But if your domain is reasonably well defined and stable, and if you have worked in it for a while, leverage it!

If it seems as if this is a lot to manage, it is. But it is still easier, and less expensive, to manage known assets than it is to discover them. Organizations and communities constructing complex systems within a domain will undoubtedly still have to consider, capture, and codify all the

aspects that are codified in a DSSA. This cost, while high, provides adequate return on investment—the goal here is to capture once, reuse forever.

The explicit capture and use of product lines is an even more business-centric practice. Product lines facilitate reuse at the architectural level, and allow organizations to construct and manage new product variants with only incremental costs. As markets diversify and organizations do business with an increasing array of cultures, countries, standards, and customer needs, being able to tailor and market a wide variety of similar products becomes increasingly important. As a side benefit, the same product line techniques can be used to help understand the evolution of individual products over time and to capture “what-if” decisions and rationale in more explicit ways, further bolstering an organization’s core business knowledge.

A caveat: domain-specific software engineering is largely a horizontal endeavor: it means surveying and unifying engineering activities across products, and perhaps even across business areas. Organizations that can adapt to this style of engineering can exploit DSSE. However, many organizations still treat product development as a series of independent ‘stovepipes,’ where personnel, engineering knowledge, and budgets are strictly partitioned across product boundaries. If this remains the case, an organization will never be able to exploit DSSE, since it cannot make the horizontal investments necessary to exploit commonalities and reuse.

## 15.6 Review Questions

1. What is domain-specific software engineering (DSSE)? What problems in software development does it address?
2. What are the three main concerns addressed by DSSE? How do they relate to one another?
3. How does DSSE help to partition problem spaces and solution spaces? How does this make software development easier?
4. Enumerate the various artifacts that are part of a DSSA. What information does each artifact contain? What is its purpose?
5. What is a reference architecture? How does it differ from an ordinary software architecture? What different kinds of reference architectures can be created?
6. When should a reference architecture be developed?
7. What is a product line? How does it differ from a domain?
8. What is a product-line architecture? What is the relationship between a reference architecture and a product-line architecture? What are variation points?

9. Identify strategies for unifying multiple related products into a product line.
10. What is the relationship between architectural design decisions, features, and products in a product line?
11. How can product lines be used to capture variations in a single product over time?
12. How can product lines be used to capture “what-if” scenarios in product development?
13. What is product line selection and how is it performed?
14. What are some strategies for unifying products with different intellectual heritage into a product line?
15. What is the relationship between DSSAs, product lines, and architectural styles?
16. How does Koala assist developers in domain-specific software engineering? What Koala features enable it to capture product line architectures?
17. How can domain-specific software engineering techniques help in the construction of software-defined radios? How can software defined radios form a product line?

## 15.7 Exercises

1. Select a problem domain with which you are familiar and try to produce a domain model as described above. Which of the domain modeling activities pose the greatest challenges? Why?
2. Survey some of the architecture-based development approaches presented in this book, and identify how (or if) they address the three primary concerns of domain, business, and technology. Is any one concern favored over others? Why?
3. Find two to four examples of systems that are in the same domain but are not built by the same organization. Create tables, like those in this chapter, showing the elements in each product, grouping them into features, and showing how features are composed into the products. Speculate on how you might use DSSE and product line techniques to unify these products into a product line, or to extract a DSSA from them.
4. Use an architecture description language that supports product-line modeling such as Koala or xADL to capture at least three different Lunar Lander games with different features.
5. Download and review the SCA specification. What aspects of a DSSA are covered by this specification, and which are not? Is it an adequate reference architecture for the domain of software-defined radios?
6. Find an open-source project that has multiple product variations—perhaps for reasons of running on different platforms, providing different services, or working in an international context. Determine how these product variants are managed. Is an architectural approach at work?

## 15.8 Further Reading

A tremendous amount of the general DSSE/DSSA information in this chapter comes from early work on domain-specific software engineering in the avionics domain by Tracz and Batory et. al. [16, 17, 285–287, 290, 291]. These references not only provide deeper background on DSSE and DSSAs in general, but also discuss yet another application domain in which these techniques have been applied. Tracz has also written extensively on reuse in general, with most of his articles compiled into his book *Confessions of a Used Program Salesman* [289].

The Koala [213] work is another excellent example of the successful use of architecture-centric development in practice. Although the early Koala work was focused on individual product lines, van Ommering has expanded his work to cut across product lines and address product populations [298] as well.

There is extensive literature on product lines. Clements and Northrop [40] write about product lines from a high-level perspective, focusing on management issues, processes, patterns of practice, and case studies. Gomaa [99] takes a UML-centric approach to modeling both product lines and patterns found therein. Pohl et. al. [229] also take a primarily process-centric approach.

Another substantial body of work on product line architectures and modeling comes from André van der Hoek et. al. in the Ménage project [245, 295, 296], which captured options, variants, and versions explicitly in architectural models and which inspired the product-line features in xADL.

## CHAPTER 16

# 16 Standards

Over the years, various organizations have attempted to create standard approaches, techniques, and tools for architecting software systems. Other standards simply emerge as a result of common use among many organizations. We have already seen some of these standards earlier in the book, such as the Unified Modeling Language (UML).

Some of these standards have achieved widespread adoption and significant backing in industry and government. They are often mandated for use on different projects. In general, these standards encapsulate a significant amount of engineering knowledge and guidance. However, it is important for software architects and other stakeholders to establish and maintain a rational perspective on these standards: what they are good for, what they can provide, and what they fail to provide. Often, the momentum behind a standard creates a (vastly) over-inflated perception of its real value and impact. The goal of this chapter is to put some of the most influential standards in context and identify their strengths and weaknesses.

### Outline of Chapter 16

- 16 Standards
  - 16.1.1 What are Standards?
  - 16.1.2 Why Use Standards?
  - 16.1.3 Drawbacks of Standards
  - 16.1.4 When to Adopt
- 16.2 Specific Standards
  - 16.2.1 Conceptual Standards
  - 16.2.2 Notational Standards
  - 16.2.3 SysML
  - 16.2.4 Standard Tools
  - 16.2.5 Telelogic System Architect
- 16.3 Process Standards
  - 16.3.1 Rational Unified Process
  - 16.3.2 Model Driven Architecture
- 16.4 End Matter
- 16.5 Review Questions

- 16.6 Exercises
- 16.7 Further Reading

### 16.1.1 What are Standards?

**Definition.** A *standard* is a form of agreement between parties.

From a software architecture perspective, there are many different kinds of relevant standards: standards for notations, tools, processes, interfaces, organizations, and so on. Standards can come from different sources: individuals, teams, single practitioner organizations, coalitions of such organizations, governments, or organizations whose specific goal is to create and codify standards such as ANSI, ECMA, ISO, or the W3C. When a standard is controlled by a body that is considered to be authoritative, the standard is often called a *de jure* standard (meaning ‘from law’). *De jure* standards often:

- are formally defined and documented;
- evolve through a rigorous, well-known process;
- are managed by an independent body, governmental agency, or multi-organizational coalition rather than a single individual or company.

Because of these characteristics, *de jure* standards tend to be the ones that are mandated for use in specific projects. The other kind of standard is a *de facto* standard (meaning ‘in fact’ or ‘in practice’). *De facto* standards often:

- are created by a single individual organization to address a particular need;
- are adopted due to technical superiority or market dominance of the creating organization;
- evolve through an emergent, market-driven process;
- are managed by the creating organization or the users themselves, rather than through a formal custodial body.

The line between a *de jure* and a *de facto* standard is not always clear. For example, HTML is a standard notation for encoding Web pages, and has all the above characteristics of a *de jure* standard, but the W3C has no authority to force individual Web publishers to follow the HTML standard (instead, market issues of browser compatibility tend to be the factor driving adoption). Similarly, *de facto* extensions to HTML have been created by companies such as Microsoft and Netscape have that are widely used simply because of their creators’ dominance in the browser market. In the computing world, popular *de facto* standards often evolve into *de*

*jure* standards: Netscape developed the Javascript Web scripting language on its own and included support in its browser. As more and more people became dependent on Javascript, Netscape relinquished some of its control over the standard and gave it over to a standards body (ECMA), where it has been standardized as ECMAScript.

Both *de jure* and *de facto* standards can be *open*, *proprietary/closed* or somewhere in between. Totally open standards allow public participation in their development; anyone is free to come in and suggest improvements or changes. Totally proprietary or closed standards mean that only the custodians for the standard can participate in its evolution. Standards bodies like ANSI, ISO, and ECMA tend to fall somewhere in the middle: some of these allow virtually open membership, while others have a higher barrier to entry (voting of the existing members or a steep membership fee, for example).

Stakeholders and architects should be keenly familiar with the state of a particular standard before adopting it by asking key questions: who supports the standard? How does it evolve? Is it dependent upon one specific company—that may be a competitor? What are its success and failure stories? How can feedback be incorporated into the standard’s future development?

### 16.1.2 Why Use Standards?

Standards can provide many different tangible benefits to their users. Many of these benefits derive from standards’ ability to create *network effects*. A *network effect* occurs when the value of a particular service or product goes up as more and more users employ it. The Web exhibits a classic example of a network effect: as more and more users publish content on the Web through the HTTP [74] and HTML [234] standards, the value of the Web as a whole increases for each of its users, since each of these users can access the new content without any additional investment.

Standards can ensure consistency across projects or organizations. Consistency is often the key driver of a network effect. Consider the value of the use of consistent symbology in a notation such as UML: as more and more stakeholders describe systems using UML, more people can develop an understanding of those systems without investing in learning a new notation.

Certain kinds of standards, such as interface or behavior standards applied to products, can be used to ensure interoperability or interchangeability. For example, the HTTP protocol can be seen as an interface standard: it dictates how to interact with a component, but not how that component must be implemented internally. Therefore, components developed by

diverse organizations can all interoperate (on some level) as long as they conform to the HTTP standard. Interchangeability is a higher level of standardization; interchangeable software components can be swapped out for one another with little or no effort. In the world of software, interchangeable parts often exhibit different quality characteristics: one may be optimized for use in a single processor system while another may be optimized for use in a distributed system.

Standards are bearers of engineering knowledge, and can carry it from project to project. Often, standards are developed because organizations continue to reinvent the same basic techniques or tools over and over again at great expense. Standards reduce costs for the entire market by collecting and making the engineering knowledge available to everyone.

Standards also serve as targets for tool vendors. Organizations that adopt widely-accepted standards will generally have the ability to buy off-the-shelf tools that implement the standard along with training supplements such as books, videos, and so on, instead of investing time and money to develop their own. For the most popular standards, adopting organizations will often have a choice of several competing tools, and market competition can drive further improvements in these tools.

Standards can also reduce the cost of powerful software tools. While software is expensive to produce initially, once it is created it can be replicated infinitely at little to no additional unit cost. In economic terms, software makes excellent use of *economies of scale*. By conforming to a standard, a tool can gain wider appeal, and thus sell more units. As more units are sold, the developing organization can amortize the initial development cost across all the units, greatly reducing the price it needs to charge to be profitable. For example, consider two software tools that both cost \$1,000,000 to produce. If one tool sells 100 copies, then the price for each unit must be above \$10,000 just to recover the development cost. However, if the tool sells 100,000 copies, then the price could drop to only \$10 per unit. A tool that conforms to a widely-accepted standard is much more likely to sell many copies than a tool that does not.

Over time, standards evolve. The procedure for evolving a standard is generally governed and managed by the standard's custodial organization, as discussed above. As standards are adopted and used, various weaknesses or drawbacks will be identified, and future versions of the standard can be developed to rectify some of them. Organizations that adopt the standard can take advantage of these lessons and the resulting improvements in the standard, without bearing the entire brunt of the costs of developing them.

Having substantial control over a widely-accepted standard can grant an enormous amount of market power to a custodial organization. If a single organization, such as a commercial company, develops a standard that becomes widely adopted, then that company has a great deal of control over how the standard is used and how the standard evolves. It can guide the standard's evolution in directions that match its own business interests—or drive it away from a competitor's interests.

Overall, the use of standards can carry many benefits. However, standards are not a panacea, and must always be evaluated with a critical eye, as will be discussed in the next sections.

### 16.1.3 Drawbacks of Standards

Above, we covered a host of benefits that can be conferred upon organizations adopting and developing standards. In doing so, organizations must work to mitigate or avoid some of their drawbacks.

The very nature of ‘standards’ is somewhat at odds with the realities of software architecture. One message that this book has attempted to convey is that stakeholder needs and desired qualities of software attributes vary widely from project to project and domain to domain. Agility is a key factor in “doing” software architecture successfully. In contrast, standards often attempt to apply the same concepts and processes to widely different development efforts. This is probably the key weakness of most architecture-related standards in use today.

A related drawback is that the most widely-adopted (and thus often best-supported) standards are those that are the most general. This should not be surprising—the adoption potential of a particular standard is proportional to its applicability. However, this means that domain-specific standards that can impart a lot of specific guidance and value to projects within a domain are often the ones that have the least support—from tools, researchers, and so on.

The primary tension in standards development exists between *overspecification*—prescribing too much and limiting the utility of the standard and *underspecification*—prescribing too little and limiting the benefits of the standard. As you might expect, the most broadly accepted standards tend to be the ones that are *underspecified*, leaving out significant semantic details. Without well-defined semantics, it is difficult to make quality judgments about a product simply because it conforms to a standard.

A related problem is the *least-common-denominator* problem. Because standards are often developed by a committee of diverse, often competing organizations, the individual goals of the organizations will tend to

diverge along many dimensions. When many organizations are involved, divergent viewpoints are often simply left out of the standard entirely, and only agreeable elements are included. When this occurs, the standards that emerge tend to be small and underspecified.

The opposite problem can also occur: when divergent opinions occur among the developers of a standard, everyone's solutions are included, usually leaving the choice of approach up to the implementer of the standard. These standards are underspecified in a different way: while there is no shortage of options for users, there is also little guidance as to which approach to choose, and fundamental benefits of using a standard such as interoperability and consistency are reduced.

**Sidebar: De Jure Standards: The “Ivory Towers of Industry”**

One critical element that distinguishes *de jure* standards from *de facto* standards is market adoption. A *de facto* standard has become a standard because it fulfills some need for a significant number of users. For these standards, market forces and network effects are primary drivers of adoption.

*De jure* standards (at least, those that have not emerged from *de facto* standards) are not similarly motivated. They are often developed and codified without pre-existing market adoption. The quality of these standards is thus brought into question—they have not competed in an open “marketplace of ideas” and thus may be inadequate solutions even for the problems they are intended to address. This mirrors a common criticism levied at academic solutions to problems: that they come from the “ivory tower”—they may be well-grounded in theory but are untested in practice. This is especially concerning when these standards are mandated for use in projects. Here, there is a significant danger that being *standards-compliant* will be more important than being *good*.

*De jure* standards usually arise from good intentions. Often, recognized experts in a particular domain are tapped to help produce the new standard. Sometimes, these standards result from composing existing *de facto* standards as well.

*De facto* standards are not a panacea either—there are many examples of *de facto* standards that have different problems—for example, poor support for evolution of the standard, or widespread adoption inhibiting innovation.

The key questions to ask about *any* standard are:

- What problem does this standard address?
- What are the limitations of this standard? (That is, what

problems does this standard NOT address?)

- Has the standard been successfully applied?
- Whether or not it has been applied, is the standard theoretically sound?
- Are the practical reasons for adopting this standard compelling?
- What benefits can be expected from using this standard? Alternatively, what work can be avoided by adopting the standard?
- Are there alternatives to adopting the standard? What are the costs and benefits of these alternatives?
- What strategy is in place for dealing with the evolution of the standard?
- What contingency plans are in place if the standard fails to evolve?

#### 16.1.4 When to Adopt

One of the critical questions that every development organization must answer when faced with a new standard is when to consider adoption. How an organization affects and is affected by a standard is largely governed by how and when they choose to adopt that standard. Both early and late adoption have advantages and disadvantages.

Some of the benefits of early adoption include:

- **Ability to influence the standard:** Early adopters can often become significant participants in the body that is responsible for creating the standard. They may then be able to move or evolve the standard in a way that is advantageous for them, or work to exclude competitors from similar participation.
- **Early to market:** If the standard becomes successful, early-adopter organizations are the first to benefit. If the standard can be leveraged in the product market, then the organization's products will be among the first to support the standard.
- **Early experience:** If the standard is successful or useful, early adopters will have more experience than others with using the standard, and can leverage this experience to their benefit.

Some of the drawbacks include:

- **Risk of failure:** If the standard ends up not being successful, early adopters can be left “holding the bag.” Investment in the standard will not pay off because the standard will not be supported.

- **Moving target:** As standards are initially developed, they go through numerous changes. Early adopters will have to adapt to these changes as they occur; if they develop products based on an early version of a standard, they may not be fully standards-compliant when the standard is eventually released.
- **Lack of support:** Early in their development, standards will not have extensive support. Certain problems may not have been ironed out. Without support, organizations may end up developing support of their own, thus negating some of the cost benefits of adopting a standard at all.

Some of the benefits of late adoption include:

- **Maturity of the standard:** Older standards tend to be more mature. They are more stable and undergo fewer changes; the changes that are made are done through a more principled process. ‘Bugs’ in the standard have likely been worked out, or at least worked around.
- **Better support:** Older standards tend to be better supported, in terms of tools, documentation, training materials, and so on. This support may be developed by other organizations, and can be bought rather than developed.

Some of the drawbacks of late adoption include:

- **Inability to influence the standard:** It is, in general, more difficult to influence a standard after it has been developed and supported for a long time. Existing organizations in the standards body will have formed a community with its own culture, and the barrier to entry into this community will gradually grow over time.
- **Restriction of innovation:** Older standards may not track cutting-edge developments in technology or methods. Becoming attached to an older standard may limit an organization’s view to innovation.

So, when should an organization adopt a standard? The answer depends on the organization’s goals. If the standard will substantially influence an organization’s core business, it is probably more useful for the organization to take the risk and absorb the costs of getting involved early. If the standard fails, then only the original investment is lost; if the standard succeeds, the organization may find itself being unduly influenced by a standard it cannot control. Alternatively, if the standard is simply a tool that the organization will use to improve its own products but will not be part of its core business, then waiting for others to ‘foot the bill’ for maturing the standard is a smarter decision.

## 16.2 Specific Standards

This section will cover many of the standard approaches to architecting software systems that are widely accepted and in use today, with an emphasis on the specific benefits and limitations of each. We will attempt to categorize each standard based on its primary purpose, but recognize that many of these standards are difficult to peg in any one category.

### 16.2.1 Conceptual Standards

Conceptual standards tend to address the range of activities that go into creating and using architecture. Because of their wide scope, they tend to provide ‘high-level’ guidance: for example, many focus on what should be documented, but not how (i.e., in what notation) it should be documented. Conceptual standards often dovetail with other, more specific standards for methods or notations to form more complete and detailed approaches to software and systems development.

#### IEEE 1471

IEEE 1471 [130] is an IEEE recommended practice for architectural description that is often mandated for use by government contractors and other organization. It recognizes the importance of architecture in helping to ensure the successful development of software-intensive systems. IEEE 1471’s scope is limited to architectural descriptions: that is, architectural descriptions can be conformant to the standard, while other artifacts (products, processes, organizations) cannot. Architectural descriptions are a collection of products used to document an architecture: in this book, we refer to these artifacts as architectural *models*. The standard itself does not describe a specific notation for these models, however. Instead, it only specifies a minimal amount of required content in the models.

IEEE 1471 takes a stakeholder-driven view of architectures, much as we have done in this book. Architecture descriptions in IEEE 1471 specifically identify system stakeholders and their concerns. A complete architectural description will address all the concerns of all the stakeholders, although in practice this is more often an ideal than a reality.

IEEE 1471 architecture descriptions are also composed of views that are instances of viewpoints. The IEEE 1471 notion of views and viewpoints is consistent with the one used in this book. As we have discussed, views and viewpoints organize the architecture according to stakeholder concerns. Just as the standard does not advocate the use of any particular notation, it also does not advocate the use of any particular set of viewpoints—adopters of the standard are expected to choose viewpoints that correspond to its stakeholders’ concerns. The standard encourages implementers to maintain consistency among views, and to document any known inconsistencies in the architecture description. It does not explain

how consistency is supposed to be accomplished or measured, or what methods should be employed to do so.

As a standard, IEEE 1471 is purposefully light on specification (it is difficult to call it underspecified because the limits of its scope are obvious and deliberate). The standard provides a good starting point for thinking about capturing architectures, and does not try to advocate a single approach for every domain. The definitions and concepts that it uses are more-or-less consistent with those found in this book.

Users must be careful not to attribute too much capability to the standard, however. Our experience is that there is a belief among many organizations that being IEEE 1471 compliant is the equivalent of “doing good architecture.” In fact, being IEEE 1471 compliant indicates that a set of ‘architecture description’ products have been developed and designated by the system’s engineers, but does not ensure that these products are of high quality, that they capture the critical aspects of the system, that they are expressed in appropriate notations, or that any reasonable methodology has been used to develop and check these products for consistency. As such, IEEE 1471’s contributions are largely conceptual.

#### **DoDAF: The Department of Defense Architecture Framework**

DoDAF [67] is a U.S. Department of Defense standard for documenting systems architectures. It is the successor to the previous C4ISR architecture framework, and supercedes it. DoDAF (and standards like it) are often referred to as ‘architecture frameworks.’ Here, ‘framework’ generally designates a process or set of viewpoints that should be used in capturing an architecture. In general, these frameworks have little to do with the architecture implementation frameworks we discussed in Chapter 9.

Like IEEE 1471, DoDAF’s contributions are mostly at the conceptual level. DoDAF more deeply prescribes what kinds of things should be captured in an architecture description. Unlike IEEE 1471, it advocates a specific approach that is more divorced from stakeholder concerns, as it identifies specific viewpoints and what sorts of information should be captured in each of them. Like IEEE 1471, DoDAF leaves many choices up to the user: for example, what kind of notation(s) to use to document the architecture views, and how to ensure consistency among them.

DoDAF terminology conflicts somewhat with the terminology used in this book with respect to views and viewpoints. The correspondence is roughly as follows:

Concept	Our Term	DoDAF Term
---------	----------	------------

A set of perspectives from which descriptions are developed	Viewpoint set	View
A perspective from which descriptions are developed	Viewpoint	(Kind of) product
An artifact describing a system from a particular perspective	View	Product

Throughout the remainder of this discussion, we will use our terminology (viewpoint set, viewpoint, and view). However, the DoDAF standard itself uses the alternative terms (view and product).

DoDAF is a multi-viewpoint approach. The various viewpoints within these sets address architectural design decisions at many levels, from the most abstract (concepts, missions) to the reasonably detailed (individual topologies of components and connectors). DoDAF viewpoints are grouped into four sets. These sets are:

**The operational view (OV):** The OV “identifies what needs to be accomplished, and who does it.” It defines processes and activities, the operational elements that participate in those activities, and the information exchanges that occur between the elements.

**The systems view (SV):** Views in the SV viewpoint set describe the systems that provide or support operational functions, and the interconnections between them. The systems in the SV are associated with elements in the OV.

**The technical standards view (TV):** The views in the TV viewpoint set identify standards, (engineering) guidelines, rules, conventions, and other documents intended to ensure that implemented systems meet their requirements and are consistent with respect to the fact that they are implemented according to a common set of rules.

DoDAF also recognizes some cross-cutting concerns that affect all views (AV). AV products include high-level overviews of the system and the environment in which the system will be deployed, and a unified dictionary that defines terms used throughout all other views.

The DoDAF viewpoints are optimized for documenting complex architectures consisting of many interconnected and communicating nodes. These architectures are often called “system-of-systems” because the system as a whole is made up of constituent parts that are themselves complex systems with their own architectures.

To illustrate how the DoDAF is used to model a system-of-systems, we present a Lunar Lander application modeled in a subset of the DoDAF viewpoints.

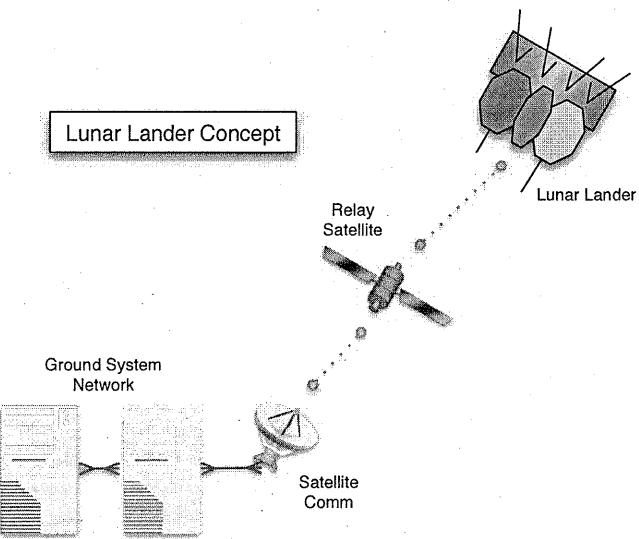


Figure 16-1. DoDAF OV-1 view of Lunar Lander

An OV-1 view is a stylized graphical representation of the system's operation. It is a free-form overview of the application and important elements in it. As noted above, the DoDAF views are not optimized for simple one-node systems like the basic Lunar Lander application we have covered in this book so far. However, in a more complex Lunar Lander system, communicating nodes such as ground stations, satellites, sensors, and so on might be depicted in such a view. Figure 16-1 shows an OV-1 view of a system-of-systems Lunar Lander example. Here, the Lunar Lander itself communicates with the ground utilizing a satellite to relay data to a satellite communication station, which in turn is connected to a ground station. This is the most conceptual and least rigorous DoDAF viewpoint; other OV products are less conceptual and more concrete.

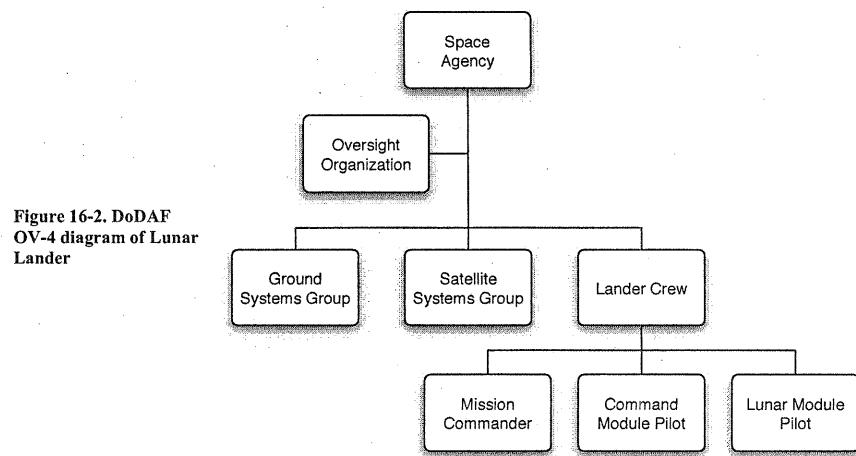
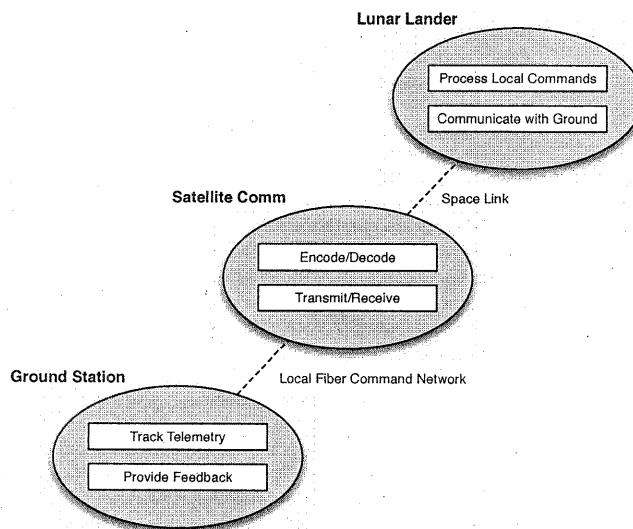


Figure 16-2. DoDAF OV-4 diagram of Lunar Lander

Figure 16-2 shows another DoDAF OV view, an OV-4 "Organizational Relationships" view. This diagram shows the relationships between various organizations and sub-organizations that are involved in a project. Here, the main space agency oversees various sub-agencies, with assistance from an oversight organization. One sub-agency, the Lander Crew, is expanded to show the individuals roles that are assigned to personnel within that sub-agency. Note that the OV-4 diagram primarily depicts the relationships between people and not technological artifacts. The blending of organizations, personnel, and technology typifies OV diagrams in DoDAF.

Figure 16-3. DoDAF SV-1 diagram of Lunar Lander



DoDAF SV views tend to be more technical in nature. Figure 16-3 shows an SV-1 “Systems Interface Description” view. The nodes are intended to correspond to nodes shown in OV diagrams. This shows an initial breakdown of functional responsibilities among the nodes, as well as the interconnections between them. Many such SV-1 views can be created for the same system, depicting the system at different levels of abstraction or showing interconnections between individual functions on nodes, rather than just the nodes themselves.

Figure 16-4. DoDAF SV-3 diagram of Lun Lander

from \ to	Ground Station	Satellite Comm	Lunar Lander
Ground Station		Ground Feedback (TCP/IP)	
Satellite Comm	Lander Transmissions (TCP/IP)		Ground Feedback (Space Protocol)
Lunar Lander		Lander Transmissions (Space Protocol)	

DoDAF makes extensive use of what it calls “matrix” views, also known as “ $N^2$ ” diagrams. These views are generally depicted as tables. Each axis of the table is populated with an identical set of nodes. These nodes generally represent concrete elements such as systems, subsystems, hosts, or devices. Each cell in the body of the table represents a possible interconnection between two of the nodes. If the two nodes are in fact connected, details about the connection are listed at the intersection cell; otherwise, the cell is left blank.

Matrix views are often directly correlated with graph (i.e., “box-and-arrow”) views of a system. Each node in the graph is listed on the axes of the table, and each line on the graph corresponds to a filled cell in the body of the table.

Figure 16-4 shows one such diagram, an SV-3 “Systems-Systems Matrix” diagram. In this diagram, the nodes on the axes are drawn from the earlier SV-1 diagram shown in Figure 16-3. Nodes on the diagonal are grayed out; communication between a node and itself is not considered. Each remaining node describes information exchange from the node named on the vertical axis to the node named on the horizontal axis. Nodes where no information is communicated, or no link exists (e.g., from the Ground Station directly to the Lunar Lander) are left blank. Here, as with other DoDAF diagrams, the amount of detail present is chosen by the user. The diagram in Figure 16-4 is relatively simple, showing only the kind of data transmitted and the protocol used. However, the DoDAF standard lists many types of information that can go in each node: status, purpose, classification level (e.g., unclassified, secret), means (e.g., the kind of network or protocol used), interface standard, and so on.

DoDAF TV products focus on identifying and tracking the technical standards that will be used to implement the described system-of-systems. DoDAF assumes that many aspects of these systems will be implemented using reusable off-the-shelf components that conform to various published standards. TV products provide ways of identifying what those standards are.

Standards for SV-1 Systems			Ground Station	Satellite Comm	Lunar Lander
Service	Service Area	Standard			
Information Technology Standards	Operating System Standard	ISO/IEC 9945-1:1996, Information Technology - Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API)	Baseline: 1 January 2007	Baseline	Baseline + 3 mos
Information Transfer Standards	Data Flow Network	Extensible Markup Language (XML) 1.0 (Fourth Edition) W3C Recommendation 16 August 2006	Baseline + 6 mos	Baseline + 6 mos	
	Physical Layer	FDDI / ANSI X3.148-1988, Physical Layer Protocol (PHY) – also ISO 9314-1	Baseline + 3 mos	Baseline + 3 mos	

Figure 16-5. DoDAF TV-1 diagram for Lunar Lander

A portion of a TV-1 diagram for the Lunar Lander is shown in Figure 16-5. The leftmost column of the table shows a number of areas in which standards apply. The second column shows sub-areas. The DoDAF, and a partner specification called the Joint Technical Architecture (JTA) enumerate these areas. Each system or subsystem, in this case drawn from the earlier SV-1 view, is associated with standards drawn from these areas. Each system or subsystem can also be given an absolute or relative timeframe in which it will comply or leverage the standard. For example, in this diagram, the Ground Station, Satellite Comm Station, and Lunar Lander are all running operating systems that conform to the POSIX standard [132]. Not all subsystems must use all selected standards, of course. Here, the Ground Station communicates with the Satellite Comm station using XML, sent over a Fiber Distributed Data Interface (FDDI) physical network. Different standards (not shown here) would facilitate the communication between the Satellite Comm and Lunar Lander subsystems.

DoDAF describes, in great detail, the breadth of information that can be captured in an architecture description. It also categorizes that information into viewpoints and, where appropriate, describes potential points of

correspondence between viewpoints. If anything, DoDAF is overspecified—including all the viewpoints and details that DoDAF describes would be overkill for most architecture modeling jobs, even in the most complex of circumstances.

While it introduces substantial complexity, this breadth is DoDAF's primary strength. In some sense, DoDAF can be seen as a huge checklist of items that may be useful to capture or think about in the development and modeling of a system's architecture. As with any modeling notation, users must decide for themselves what kinds of models to create, at what levels of detail, and so on. The DoDAF offers some advice in this regard, discussing different uses for architecture models and the viewpoints that are (in whole or in part) applicable to that use. However, even with this advice, users must still decide how they want to use the DoDAF on a case-by-case basis.

DoDAF does not, in general, mandate any particular method or notation for documenting the various viewpoints. Therefore, its users can choose any subset of the viewpoints they want, and document them using any notation or tool they want. To its credit, the DoDAF specification provides examples for each viewpoint, including UML examples. However, these examples rarely exercise all possible details that can be captured in a view. Following the examples too closely would result in a set of views that left out major details. To strengthen the connection between DoDAF and UML, the OMG has submitted a request for proposals for DoDAF UML profiles [212]. However, UML is not ideal for all DoDAF viewpoints (UML has no tabular diagram that would work for the matrix viewpoints, for example). Users must select notations and then weigh the advantages and disadvantages of their selection. Choosing several notations will increase the difficulty of coordinating them. Selecting a single notation might leave out important details, or make some viewpoints cumbersome.

**Takeaways:** Compared to the leanness of IEEE 1471, DoDAF takes the same high-level approach but goes into much more detail. It is optimized for capturing the relationships between people, organizations, system design decisions, and technical standards for complex and composite systems. It provides users with an extensive amount of information about *what* sorts of things to capture when developing an architecture, but far less information about *how* to capture that information or evaluate the results. Additional extensions to the standard, such as the aforementioned mapping of DoDAF views to UML, can fill in this gap. Because of the wide scope of the standard, it may be difficult for users to identify which views are important to capture for a particular system. Because of its specificity, it may give users a false sense of security—that everything has been covered when in fact there are some stakeholder concerns that are being short-changed. A remedy for this is to focus first on stakeholders

and concerns (as IEEE 1471 suggests) and then identify which DoDAF views map onto these concerns.

#### TOGAF: The Open Group Architecture Framework

The Open Group Architecture Framework (TOGAF) [282] is an enterprise architecture framework that is the product of an iterative collaborative effort by members of The Open Group, a collection of more than 200 companies and other organizations. TOGAF is an “enterprise architecture framework;” as such it takes into account concerns beyond just hardware and software, such as human factors and business considerations. Enterprise architectures tend to focus on organization-wide solutions to implement business goals. Elements in an enterprise architecture might include databases, applications like spreadsheets and Web browsers, various client and server machines, as well as people in various roles. TOGAF borrows concepts and terminology from IEEE 1471; its notions of architecture, views, viewpoints, and so on are consistent with those discussed above in the context of IEEE 1471. Additionally, TOGAF focuses on architectural aspects beyond hardware and software, taking into account human factors and business considerations. Various versions of TOGAF have been developed over the years; each version has grown to encompass more aspects of architecture. TOGAF version 8 encompasses:

- **Business concerns**, which address business strategies, organizations, and processes;
- **Application concerns**, which address applications to be deployed, their interactions, and their relationships to business processes;
- **Data concerns**, which address the structure of physical and logical data assets of an organization and the resources that manage these assets; and
- **Technology concerns**, which address issues of infrastructure and middleware.

TOGAF consists of three major elements: an architecture development process called the ADM (architecture development method), a “virtual repository” of architecture assets (e.g., models, patterns, architecture descriptions) extracted from architectures developed in practice, called the Enterprise Continuum, and a resource base consisting of guidelines, templates, background information, and so on to assist enterprises in following the ADM.

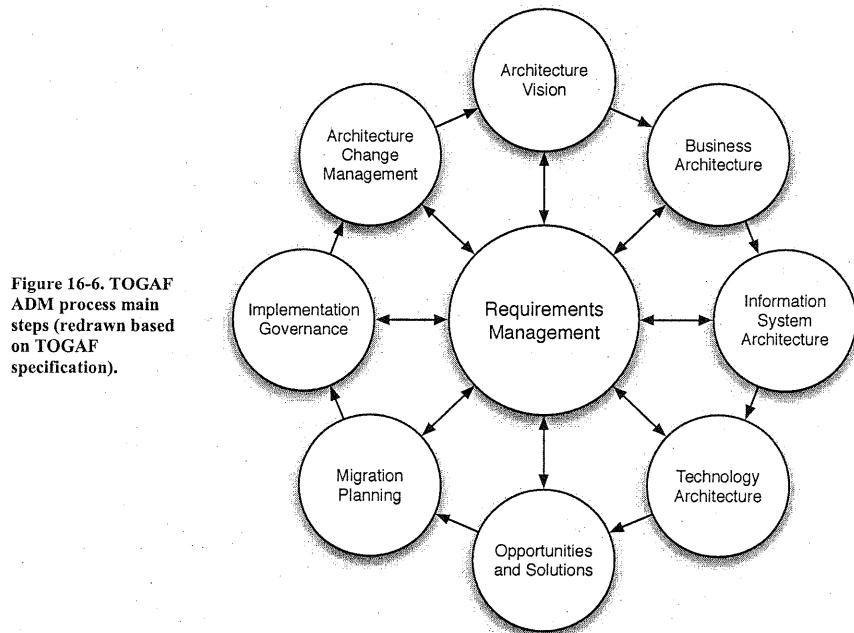


Figure 16-6. TOGAF ADM process main steps (redrawn based on TOGAF specification).

The centerpiece of TOGAF is the ADM, a process for developing enterprise architectures. Like many other modern software processes such as spiral model-based processes [21] and RUP [159], ADM is iterative, meaning that activities are visited and revisited, with each subsequent iteration refining decisions made in earlier iterations. It recommends a sequence of steps and activities that should be taken, but leaves much up to the implementing organization—how to scope the project, how to make decisions within those phases, and so on. As shown in Figure 16-6, there are 8 primary phases of the ADM, beginning with architecture vision (which is an effort to lay out what will be done and align the organization with those goals). Subsequent phases proceed through the elaboration of various architectural concerns including those identified above, creating models along the way. For each concern, different views are prescribed as ways to capture aspects of those concerns. Some of those views map naturally onto, e.g., UML diagrams, while others are defined more generally, similar to DoDAF views. Remaining phases focus on issues surrounding reduction to practice, and the implementation of the decisions that were made in earlier phases. Technologies are selected,

implementation projects are prioritized, and actual implementation efforts are managed, all of which are done in the context of the organization's assets, personnel, and capabilities. The final phase, architecture change management, addresses assessment of previous efforts and deciding how and whether to proceed through another iteration of the process.

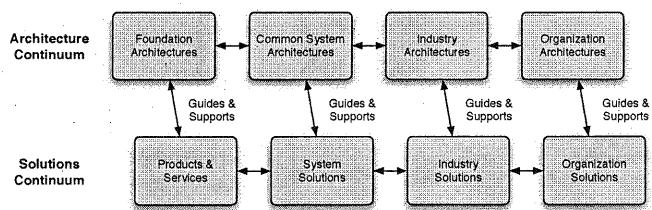


Figure 16-7. TOGAF Enterprise Continuum

The second major part of TOGAF is the “Enterprise Continuum.” The Enterprise Continuum acts as a repository of assets—of both architectural resources and known solutions. As such, it consists of two portions: the Architecture Continuum and the Solutions Continuum, as shown in Figure 16-7. Roughly, elements on the left side of the continuum are more technological and concrete; elements on the right side address business and organizational issues. Through the TOGAF Technical Reference Model and Standards Information Base, the TOGAF standard itself taxonomizes various types of components, services, and standards that can be found across the enterprise continuum. These include everything from command-line interpreters to programming languages to electronic mail and configuration management systems.

The third major part of TOGAF is the TOGAF resource base, which is a collection of useful information and resources that can be employed in following the ADM process. It includes advice on how to set up boards and contracts for managing architecture, checklists for various phases of the ADM process, a catalog of different models that exist for evaluating architectures, how to identify and prioritize different skills needed to develop architectures, and much more.

TOGAF is distinguished from other approaches by its large size and broad scope; the summary in this section only covers the major elements of the standard. TOGAF’s focus on enterprise architectures means that it addresses architecture from a different level than, for example, UML. Elements in TOGAF architectures tend to be organizations, people, and large-grained assets (applications, platforms, machines, enterprise-wide services, and so on). Otherwise, TOGAF collects a large and diverse set of “best practices” for architecture. It prescribes not only an architecture

development process, but defines a wide variety of views and concerns as well as solution elements that can be used to satisfy those concerns.

**Takeaways:** TOGAF complements other architectural approaches by taking into account more business and organizational concerns. Its high-level approach, focusing on enterprise architecture, means that it is best used for dealing with coarse-grained elements and assets, constructing entire information systems and not just software applications. Like DoDAF, TOGAF provides a substantial set of ‘best practices’ to follow and checklists to use for assessment, but individual users are responsible for the details. Following TOGAF helps to ensure thoroughness, but not necessarily quality.

#### RM-ODP

RM-ODP [136] is an ISO standard for describing open distributed processing (ODP) systems. Although the characteristics of ODP systems are described over several pages of the RM-ODP standard, they can generally be described as information systems developed to run in an environment of independent, heterogeneous processing nodes connected by a network. Primarily, the RM-ODP standard defines five viewpoints and describes associated viewpoint languages for documenting the architecture of an ODP system. These viewpoints are (descriptions copied from the specification):

**Enterprise:** A viewpoint on the system and its environment that focuses on the purpose, scope and policies for the system.

**Information:** A viewpoint on the system and its environment that focuses on the semantics of the information and information processing performed.

**Computational:** A viewpoint on the system and its environment that focuses on distribution through functional decomposition of the system into objects which interact at interfaces.

**Engineering:** A viewpoint on the system and its environment that focuses on the mechanisms and functions required to support distributed interaction between objects in the system.

**Technology:** A viewpoint on the system and its environment that focuses on the choice of technology in that system.

These viewpoints (and their associated languages) have various levels of concreteness. The computational and engineering viewpoints are more concrete and thus more constrained, since they have the goal of helping to guarantee interoperability and portability of components. The enterprise and information viewpoints are more general, and therefore their languages are less constrained.

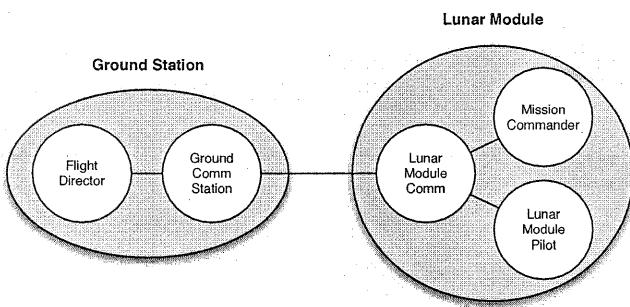


Figure 16-8. Sample RM-ODP Enterprise view

Figure 16-8 shows a sample RM-ODP enterprise view. Enterprise view elements include personnel and high-level application components, reminiscent of the kinds of elements addressed by TOGAF. The enterprise viewpoint looks at the system holistically, in terms of overall scope and its place inside the larger organization. Enterprise views can also describe agency boundaries—boundaries of responsibility or control.

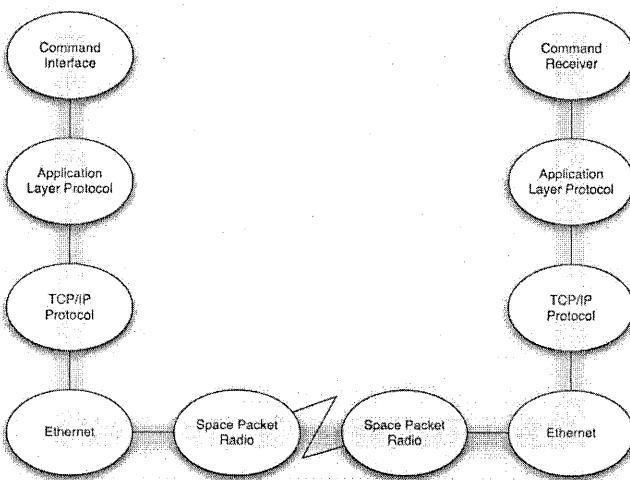


Figure 16-9. Sample RM-ODP Engineering view

In contrast, Figure 16-9 shows an example RM-ODP engineering view. This view shows how a ground system might communicate with a Lunar Lander via a complex communication channel implemented by two

communicating network stacks. Here, the elements are more technologically-oriented, and human elements do not appear. In general, both these views would be accompanied by text, explaining the diagrams, the various elements, and their interconnections. The notation used above, with ovals and interconnections, is used in the RM-ODP specification but is not canonical; many different notations (including, for example, UML diagrams and symbols) could be used to draw these diagrams.

Like DoDAF and TOGAF, RM-ODP focuses on *what* kinds of things should be modeled in an architecture, but not specifically *how* those things should be modeled. RM-ODP goes a step further than these two standards, however: instead of prescribing a particular notation for each viewpoint, the RM-ODP specification prescribes a number of characteristics that a notation describing the viewpoint must meet. Therefore, RM-ODP viewpoint languages are not languages in the traditional sense, but rather sets of requirements for a language. RM-ODP does include a separate specification describing, at a very high level, how various formal specification languages (e.g., LOTOS [135], Z [264], SDL-92 [278]) could be used to describe architectural semantics for RM-ODP architectures. The way it does this is primarily by listing an RM-ODP concept, and then identifying a formal specification language concept that could be used to implement that concept. This level of correspondence is not enough to give users serious guidance as to how to leverage these formal specification languages to implement RM-ODP.

**Takeaways:** As a standard, RM-ODP is very similar to DoDAF, although the number of viewpoints is more limited and focused. Like DoDAF, an architecture specified according to the RM-ODP standard may or may not achieve certain qualities; the primary value added by RM-ODP is to ensure that architects think about and document certain aspects of architecture that impact various qualities—distributability, interoperability, and so on. It is eventually up to the architects to actually assure those qualities. Although some mappings between RM-ODP concepts and formal methods are specified, there is a large gap between them that must be bridged by individual users. This gap is too large to assert that RM-ODP is particularly supportive of formal analysis activities.

### 16.2.2 Notational Standards

Notational standards define standard notations for writing down design decisions. Notational standards can be used to realize/implement certain elements of conceptual standards; for example, a notation like UML can be used as a way of documenting the various DoDAF views. In a way, any codified architecture description language, such as those surveyed in Chapter 6, could be viewed as a *de facto* notational standard. In this section, we examine notations that have actually gone through a

standardization process or committee and that have gained notoriety or use because they are standards.

### UML – The Unified Modeling Language

We have covered various aspects of UML [24] throughout earlier chapters of this book: its notation, its visualizations, its metamodel [211], etc. As we have seen, UML embodies a wide variety of concepts that can be used to capture various aspects of software architecture. UML includes static diagrams, dynamic diagrams, composite diagrams, and so on. This section will focus on UML as a standard, and describe its advantages and disadvantages from that perspective.

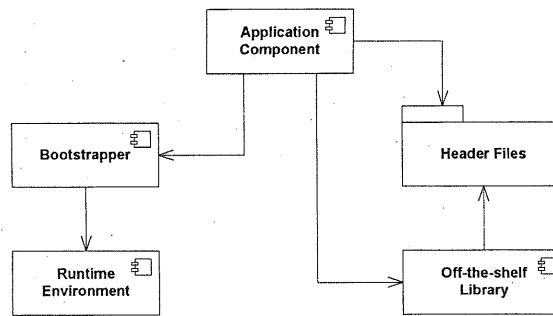
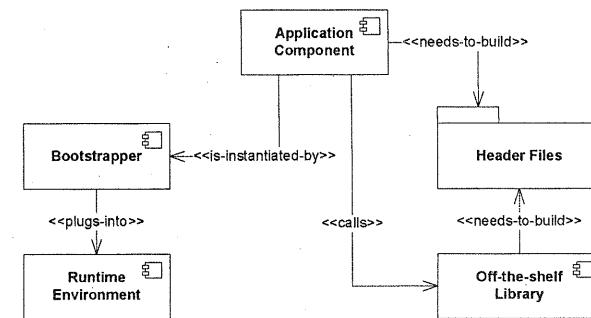


Figure 16-10. UML diagram without profile

UML provides a standard *syntax* for describing a wide variety of aspects of software systems. Basic UML (without extensions) prescribes very few semantics to go along with this syntax. It is possible for the same element or diagram to mean entirely different things. For example, the dashed arrow connector in UML indicates a dependency between two linked elements. That dependency could mean “needed to build” or “plugs-into” or “calls.” There is no way, without additional context or information, for a stakeholder to look at a dependency arrow in UML and have any clear idea what it means. This situation is depicted in Figure 16-10—the dependencies are all specified but the reader knows little about them. As such, basic un-extended UML provides little value to users, except for establishing a common symbolic representation of elements. The fact that a system is described in UML implies little about the quality of that system.

Figure 16-11. UML diagram with profile



UML’s value can be substantially increased through the use of UML extensions and profiles. UML stereotypes allow users to specialize existing UML symbols to add project or domain-specific semantics. Through stereotypes, it is possible to create specific instances of the dependency arrow that mean <<calls>> or <<needed-to-build>> or <<plugs-into>>. For example, Figure 16-11 shows the same UML diagram as Figure 16-10, except the dependencies are stereotyped. This diagram is much more readable and provides substantially more information. To be fully useful, however, a UML profile for a project must be accompanied by detailed documentation explaining when and how to use the various stereotypes, tagged values, and constraints, as well as their meaning. With the proper use of profiles, a UML description becomes a valuable tool for stakeholder communication and system understanding, and also has positive impacts on traceability and analyzability.

Even with profiles, however, UML and its accompanying tools are (currently) not well-suited to the verification of specific quality properties. Will the described system satisfy its requirements? Be efficient? Be cost-effective? Be free of deadlock? To determine answers to questions like these, additional methods above and beyond UML, ranging from inspections to testing to formal verification, must be integrated into the development process separately.

**Takeaways:** UML is not a panacea for architecture-based software development. UML provides a set of common, symbolic notations for architects to write down and communicate certain kinds of design decisions. The diagram types that have been provided in UML allow architects to model a wide variety of concepts, although there are certainly architectural design decisions that cannot be easily captured in UML. UML profiles should be used to improve the rigor and understandability of

UML diagrams, but profiles have their limits. Profiles can only decorate existing diagrams; they cannot create entirely new diagrams. Modeling a system in UML makes few guarantees about that system—UML can be used to document both good and bad architectures (although in theory, UML makes it easier to understand, communicate about, and evaluate architectures).

### 16.2.3 SysML

Despite the wide variety of modeling concepts embodied in UML, different engineering efforts require even more modeling breadth than UML has. The quintessential example of this is SysML [269]. SysML is an effort by a coalition of more than twenty engineering organizations (primarily corporations, but also universities and other organizations) [270] to customize UML for systems engineering. With respect to standardization, the SysML community has taken an interesting two-pronged approach. One group is developing and promulgating an “open-source” version of the SysML standard under a license that allows users to redistribute and modify SysML on their own. From this open-source version, an official OMG standard version of SysML has been created. “OMG SysML” is trademarked and evolves, like UML, through the standards committees and processes of the OMG.

Many individuals and organizations perceive UML to be too “software-biased” for modeling systems engineering concerns that include elements like hardware, networks, development organizations, and so on. Of course, many UML diagrams can be interpreted in ways that do capture these concerns (for example, a traditional systems engineering ‘block diagram’ closely resembles a class diagram in many ways), SysML reused parts of UML. SysML includes a subset of UML, but also extends it. Diagrams reused from UML are the activity, class, composite structure, package, sequence, state machine, and use case diagrams. Two of these diagrams are renamed for SysML: class diagrams are called “block definition” diagrams and composite structure diagrams are called “internal block” diagrams. SysML also adds stereotypes to UML as well as two new diagram types: requirement and parametric diagrams. Requirement diagrams show system requirements and their relationships with other elements. Parametric diagrams show parametric constraints between structural elements, which are useful for performance and quantitative analysis.

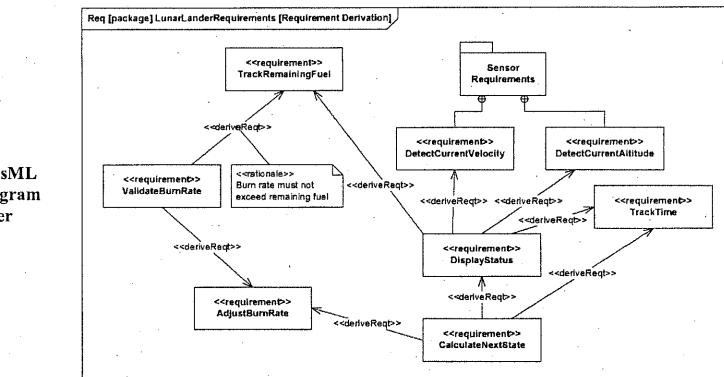


Figure 16-12. SysML requirement diagram for Lunar Lander

Figure 16-12 shows a SysML requirement diagram for the Lunar Lander application. This diagram shows only requirements and their relationships; a more complex requirement diagram might actually include additional detail for each requirement such as the actual text describing the requirement, a unique ID, and so on. Requirement diagrams can also be used to associate requirements with elements from other diagrams such as use cases. Syntactically, requirement diagrams primarily reuse and specialize elements from class diagrams, using stereotypes on classes and relationships to make those elements specific to requirement diagrams.

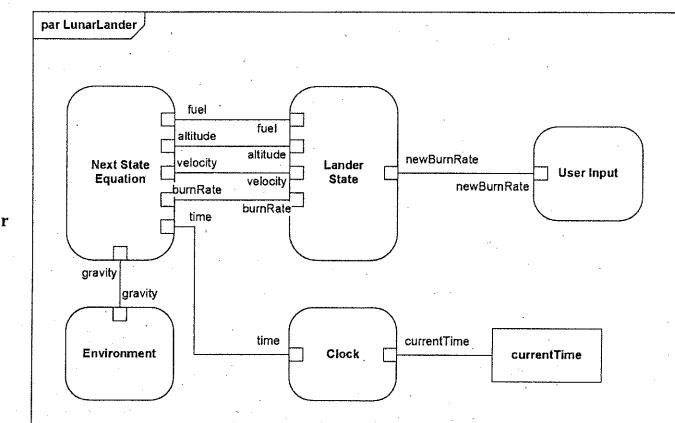


Figure 16-13. SysML parametric diagram for Lunar Lander

Figure 16-13 shows a SysML parametric diagram. Parametric diagrams are specializations of SysML internal block diagrams—composite structure diagrams in UML. These diagrams allow architects to associate quantitative parameters with various model elements. These parameters can then be associated with mathematical models, equations, or analysis techniques that can be used to evaluate or assess parts of the system quantitatively. For example, several state-storage elements (the clock, the lander state) provide values to the next-state equation, which is used to calculate the next state of the Lunar Lander simulation.

The development of SysML is consistent with our earlier assertion that UML is not necessarily a complete solution for architectural modeling. The SysML developers left out certain UML diagrams they felt were extraneous or unnecessary, and added new diagrams that were missing. SysML has not been as universally supported or adopted as UML, despite the fact that it is not a radical departure from traditional UML 2. Tool support in the form of modeling environments, for example, has lagged behind UML, and while some UML modeling environments such as Telelogic Rhapsody have some explicit SysML support, many others do not. This indicates that even a large group of influential organizations cannot necessarily force the adoption of any particular standard. Note also that even the new SysML diagrams reuse and overload existing UML symbols, likely in an effort to provide some degree of modeling support with tools that are not SysML-aware.

**Takeaways:** SysML is an example of how standards can evolve, change, and fork apart. By reusing substantial parts of the UML standard, the SysML partners were able to save a tremendous amount of effort as well as allow users to apply their existing UML knowledge in a systems engineering context. However, the changes and extensions they made to UML—conservative as they are—have been a double-edged sword. On one hand, they provide increased expressiveness for systems engineers. On the other hand, they have reduced the amount of tool support that exists for the language. Even standards that are supported by a substantial amount of influential organizations must still win many hearts and minds on technical and business merit to achieve widespread success.

Chapter 6 described two modeling languages, AADL [73] and ADML [262], from a technical perspective. However, these two modeling languages are also standards—AADL is standardized by the Society of Automotive Engineers (SAE) and ADML is standardized by the Open Group. Both standards describe new, stand-alone notations that can be used to model architectures. AADL is becoming increasingly successful, while ADML has effectively failed. Why? The answer is not necessarily clear or simple; many related factors are interacting here.

#### Sidebar: A Tale of Two Standards

AADL is a complex language. It has a rich syntax and, to an extent, graphical visualizations are still being developed. However, the primary motivation for adopting AADL is that it provides compelling analysis capabilities and tools that are not easy to obtain with other notations or approaches. It is not just a minor tweak to an existing notation such as UML. AADL's developers have begun by focusing on a community of users known to need its unique capabilities—systems engineers in the automotive and avionics domains, and others working with embedded, real-time system development. Leveraging the existing support and user community of UML is also part of the AADL strategy; a UML profile for AADL is being developed and refined. In AADL's case, standardization is only a small part of why AADL seems to be winning hearts and minds. Providing novel capabilities, making judicious use of other standards, and targeting a specific community of users with needs that match AADL's unique capabilities are all influencing AADL's growth.

ADML, compared to AADL, is relatively simple. From a technical perspective, it combines the core concepts of Acme with a few innovations in types and meta-properties and the benefits of using XML as a meta-language. As a standard, ADML failed to achieve widespread adoption, and anticipated tool support and interoperability never emerged. It is difficult to say what the reasons for this are. Unlike AADL, ADML's improvements over previous technologies are incremental. ADML was not targeted at a specific domain or user community, although some ADML documentation notes its usefulness in enterprise architecture modeling and points out deficiencies in UML in this regard. As with AADL, standardization plays only a partial role in the story behind ADML's lack of adoption and evolution. A complex array of factors contributed: a small user community without a substantial demand, the availability of contemporary alternatives such as Acme, Darwin, and xADL 1.0, lack of initial tools to help motivate community growth, and so on.

On a positive note, however, many of the concepts of ADML did eventually appear in UML 2 (and thus also into XMI). UML already had a huge userbase, and these contributions shored up support for structural modeling that was considered to be a deficiency of UML 1.x. The ideas of the ADML standard were much better received when they became part of UML. Of course, defining a new standard like ADML is much easier than convincing the already-mature UML community to incorporate these new ideas. For modest, incremental improvements, this may be plausible, and certainly ADML's contributions were a natural fit, addressing well-known drawbacks of UML. Incorporating a complex standard with many new and conflicting ideas like AADL into UML would likely cause much more

friction in the UML community, and may be infeasible.

There are several lessons to be learned from the AADL and ADML experience. Standardization alone does not ensure the success of an approach. Success is largely dependent on the size and passion of the user community surrounding the approach, and standardization is just one way to catalyze the development of a community. Another important element is to ‘prime the pump’ with support for the standard: developing initial tools, documentation, and training for a standard, even if they are not perfect, can entice early adopters much more than a simple specification. For incremental improvements, or improving deficiencies in an existing standard, it is often best to focus efforts on improving or evolving the existing standard rather than trying to develop a new, parallel standard.

#### 16.2.4 Standard Tools

Many organizational cultures will standardize on a particular tool as much (or more) than on more abstract approaches. Corporations often evaluate a spectrum of tools and then purchase one (or a small number) of them in bulk, and that tool becomes mandatory for use within the company...

##### Standard UML Tools

The wide adoption of the UML standard generally induces organizations to adopt one or more standard tools for working with UML. This is often motivated by a desire for consistency across an organization, as well as market pressures: organizations buying tools from a single vendor can often get volume discounts as well as negotiate enhanced support agreements. UML itself, however, is not bound to any particular tool. Tools that have become *de facto* standards for UML editing include IBM’s Rational Rose [237], Microsoft Visio [193], Telelogic System Architect [279], ArgoUML [2], and others.

These tools vary in their exclusivity of support for UML. Tools such as ArgoUML and Rose focus their support almost exclusively on UML, while tools such as Visio and System Architect support diagrams in many notations. All the tools support the creation and manipulation of UML diagrams, generally through a point-and-click graphical interface. The form of this interface—what menu options are available and so on—depends on the individual tool. UML does not standardize how users are to interact with these diagrams. For example, Rose uses a tree-based view organizing artifacts and diagrams within the model, and property sheets that are used to decorate various model elements.

The tools differ widely in their support for additional capabilities beyond plain UML modeling. This includes design aids, artifact generation, and

constraint analysis. Sometimes, third parties will create plug-ins for the tools that add additional features.

A generic diagramming tool such as PowerPoint can be (and often is) used to create UML diagrams, even though it has no specific understanding of UML’s (graphical) syntax and semantics. These tools, then, cannot provide any guidance to UML users to help create consistent or complete documents. UML-aware tools, on the other hand, provide design guidance as users create and edit UML. These features include:

**Support for UML’s built-in extension mechanisms:** Recall that UML profiles allow users to specialize elements and introduce additional commonalities among them. UML tools may allow a user to define stereotypes and manage associated tagged values, applying the stereotype’s tagged values to all elements of the stereotype, for example. The user interface may also provide new options when stereotypes are applied: the visual appearance of an element may change (adding an icon, for example), and new options may be presented to the user to manipulate the properties associated with that stereotype.

**Support for consistency checks:** The ability to specify and automatically check constraints can increase stakeholders’ confidence in the quality of the architecture. Most UML tools guide the user in making syntactically correct UML documents. The syntactic constraints of UML are generally basic well-formedness checks—that links have valid endpoints, or that two elements do not have the same name, for example.

Many tools go further, and allow the user to check semantic and cross-diagram consistency constraints. For example, a tool may warn a user when a sequence diagram indicates an invocation on an object whose class does not implement a method with the same name as the message. Not all of these constraints are necessarily part of the UML standard, but they are commonly-accepted conventions about particular relationships in UML and help to increase the internal consistency of UML models and reduce modeling errors. One danger in this regard is that users of a particular tool may not be able to easily distinguish which constraints are part of UML itself, and which are just being enforced by the local tool.

Beyond these generic syntactic and semantic checks, UML includes a constraint language, OCL [303], that allows users to specify constraints on UML elements and element relationships. Tools are available that can assist users in specifying OCL constraints, and then check them automatically. UML does not mandate the use of OCL as its only constraint language, however, so it is possible for UML tools to incorporate additional constraint languages.

**Generation of other artifacts:** UML models can be used as the basis for generating artifacts useful in other lifecycle activities, such as implementation or testing. Some UML tools include facilities for generating these artifacts, or parts of them. For example, Rose has an internal tool called SODA that focuses on the generation of other artifacts from Rose models. SODA effectively transforms UML models into other formats using user-definable templates. Different templates will transform UML models into different kinds of artifacts: one template may output documentation in document form in a Microsoft Word file; a different template may take the same UML model and generate code skeletons for each of the defined classes. Auto-generation of artifacts that are important in non-design phases of the software engineering lifecycle (such as code artifacts for the implementation phase) is especially useful in preventing architectural drift and architectural erosion.

**Generation of UML:** Some UML tools can take other artifacts (usually implemented systems) and automatically generate partial UML models for them. For example, some tools can iterate over a series of Java classes and automatically generate a corresponding class diagram. These inferences are not always 100% correct or useful. They may fail to make inferences about dependencies between classes because a mechanism such as dynamic classloading or reflection is used. They may also generate every class dependency, when only some of them are architecturally important. For this reason, auto-generated UML needs to be reviewed and ‘tuned’ by hand.

**Traceability to other systems:** Generation is not the only connection that UML tools may use to interoperate with other artifacts; traceability and links can be used as well. Linking mechanisms may be provided to relate UML elements with system requirements in a requirements management environment like Telelogic DOORS [1], with configuration management repositories, with code-based integrated development environments, with simulation environments, and so on. When such links are available, additional consistency constraints can be checked as well. This can extend the scope of a UML modeling environment beyond UML itself, and incorporate other architectural (and non-architectural) concerns into the modeling process.

**Takeaways:** UML tools have a profound affect on how users experience modeling in UML. While all tools provide basic support for drawing UML diagrams, the real value in the tools often comes from features provided above and beyond basic drawing: checking additional constraints above and beyond ‘plain’ UML, customizability, generation of other artifacts, reverse engineering code, traceability to other artifacts managed in different environments, and so on. These features generally automate processes that would otherwise be tedious, manual, and error-prone. It is

important to be cognizant of any differences between the UML language and peculiarities or limitations introduced by specific UML tools. Also, UML tools may lag behind the latest developments in the UML standard itself.

### 16.2.5 Telelogic System Architect

Telelogic System Architect (formerly Popkin System Architect) [279] is a popular tool among system engineers. It is used to manage diagrams of many different views of a system in multiple diagrammatic styles. It has support for more than 50 different types of diagrams drawn from different modeling methodologies—all the UML diagrams, IDEF, OMT, generic flowcharting, and more. Beyond the basic System Architect tool, a number of variants are also marketed: for DoDAF, for Service Oriented Architectures, for designing enterprise-resource planning (ERP) systems, and so on.

System Architect can support this wide breadth of diagram types because of its internal construction. Internally, diagram data is stored in a relational database that is updated as the user creates and manipulates diagrams. Each diagram type is associated with a particular vocabulary of symbols and interconnections, as well as constraints that assist the user in creating syntactically correct diagrams.

System Architect is an example of a ‘standard’ tool that trades breadth for semantic strength. It can be viewed as a very good domain-specific diagram editor. That is, it has specific support for drawing diagrams with the syntax of UML, or IDEF, or OMT, or any number of other types of diagrams. However, it has little (if any) understanding of the semantics of these diagrams. The specialized versions of the product (e.g., System Architect for DoDAF) have some additional semantic knowledge built in—such as the ability to generate or check the consistency of different diagram types.

**Takeaways:** Telelogic System Architect is a de-facto standard, flexible drawing tool that gives users a plethora of diagram types in which to express architectural decisions. On one hand, the construction of the tool makes it very easy for Telelogic to incorporate new diagram types or adapt to new diagrammatic languages and standards that emerge. However, this comes at the cost of having more limited associated support for the semantics of those notations. It is certainly easier to draw diagrams with complex syntactic vocabularies than a completely generic tool like PowerPoint, but it provides little guidance to users as to the quality, correctness, or consistency of their architectures.

## 16.3 Process Standards

The standards we have covered thus far are mostly related to how to capture an architecture, either conceptually, in a specific notation, or using a particular tool. Process standards dictate the process—that is, the steps—that are used to develop software. These standards focus less on artifacts and more on the methods used to create them.

### 16.3.1 Rational Unified Process

The Rational Unified Process (RUP) [159] is a standard that was created by the Rational Software Corporation, now IBM. Fundamentally, the RUP is an iterative process, and is inspired by Boehm's spiral model [21]. Rather than prescribing a single, concrete sequence of steps to follow when developing software, the RUP is an adaptable process *framework*, intended to encompass many different iterative processes and to be tailored for each of them. RUP describes software construction as a whole and is not focused primarily on architectural development (like TOGAF's ADM).

A RUP project is done in *phases*. The RUP identifies four specific phases:

**Inception Phase:** The inception phase includes initial activities that determine the goals and success criteria for an iteration; it includes making a business case, describing basic use cases, assessing risks, establishing budgets, and so on.

**Elaboration Phase:** Here, use cases are further elaborated and architectural design decisions are made to satisfy them. Business plans and risk assessments made in the inception phase are refined and revisited. Prototypes may be developed.

**Construction Phase:** This phase largely encompasses the implementation and construction of elements that are designed and specified in the elaboration phase.

**Transition Phase:** In this phase, the developed product is transitioned to the end users. It is validated and tested, and its functionality and quality are assessed against the goals set in the inception phase. Installation and training are performed in this phase.

The goal of each phase is to reach a *milestone*. For example, the inception phase ends with the “Lifecycle Objective Milestone,” which requires stakeholder agreement on scope, cost, and schedule, elaboration of high-level use cases, agreement on credible risk assessments, and so on. Internally, each phase consists of smaller activities apportioned to various personnel. These activities are broken up by *disciplines* such as requirements, design, implementation, testing, and so on. Iterations of these activities occur within each phase. While the inception phase is

expected to be short and is usually done in a single iteration, the other phases often involve multiple iterations.

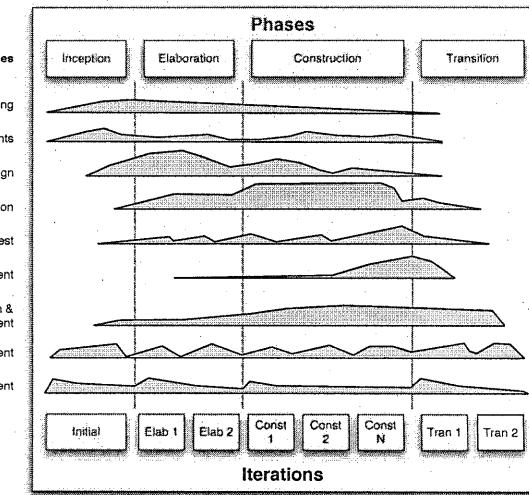


Figure 16-14. Rational Unified Process phases, iterations, and disciplines.

Figure 16-14 shows the relationship between phases, iterations, and disciplines in RUP. Time proceeds from the left to the right in the graph. Note how the development effort is partitioned by the phases and iterations occur within each phase. The dotted breakpoints between the phases indicate milestones that must be reached. Although all disciplines may be addressed during each phase/iteration, some disciplines are more prominent than others in different phases. For example, very little implementation occurs in the inception phase (perhaps proofs-of-concept or initial prototypes), while a large amount occurs during the construction phase. Likewise, requirements are a heavy focus during inception but are only revised and refined during the construction phase.

**Takeaways:** Ever since the development of the spiral model, software engineers have recognized that the use of iteration and risk analysis are important. RUP is a meta-process or process framework in which many iterative (and linear) processes are instances. For example, one could view the traditional waterfall model as a single-iteration instance of RUP. RUP has a tendency to view architecture as a design artifact, rather than as a pervasive discipline—as we have advocated in this book—but the two notions are not entirely incompatible. RUP is not necessarily a universal

meta-process; certain development strategies such as Extreme Programming or Domain-Specific Software Engineering may have more lightweight and fluid processes that do not fit naturally in a structured, iterative RUP model.

### 16.3.2 Model Driven Architecture

Model-Driven Architecture (MDA) [199] is a methodology standardized by the Object Management Group (OMG), the same body that manages the UML standard. MDA aims to reconceptualize system development by leveraging the development of models that are refined, through a series of transformations, into implemented systems. Confusingly, the word ‘architecture’ in Model-Driven Architecture does not refer to the architecture of the system under development, but rather the architecture of the various standards and languages that are used to implement the MDA approach. Synonyms for MDA include Model-Driven Development (MDD) and Model-Driven Engineering (MDE), although ‘MDA’ is generally used to refer to the OMG approach.

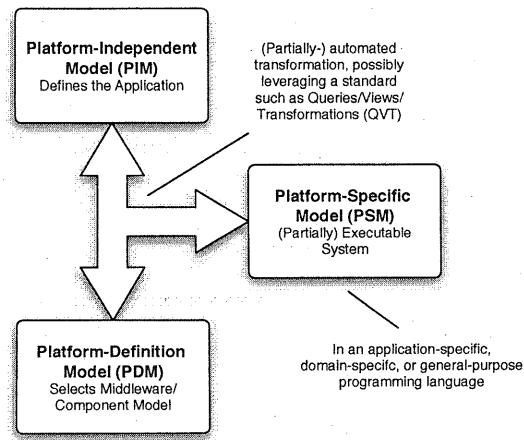


Figure 16-15. High-level overview of MDA

Figure 16-15 shows a high-level overview of MDA. In MDA, systems start out by being described in platform-independent models (PIMs). These PIMs describe the application without binding it to specific implementation technologies; any number of languages may be used for this purpose, particularly domain-specific languages. Then, a platform-definition model (PDM) is used to specify the target platform for system implementation. This may be based on some middleware or component-

based implementation technology such as CORBA, .NET, JavaBeans, and so on. By combining the application knowledge in the PIM with the platform knowledge in the PDM, one or more platform-specific models (PSMs) are created. These PSMs are part of a system implementation in a domain-specific implementation language or a general-purpose programming language like C or Java.

Ideally, once the PIMs and PDMS are defined, the rest of the translations can occur using (or at least leveraging) automated translation tools. The separate OMG QVT (Queries/Views/Transformations) standard is one way of defining model transformations. Assuming the translations are correct and preserve salient properties, the result of MDA should be a system that is faithful to the original models and desires of the stakeholders.

**Takeaways:** As a general approach, MDA is compatible with many of the mechanisms and ideas espoused in this book. For example, Chapter 9 on implementation discusses how generative technologies can be used to automatically generate (partial) implementations from architectural models, especially when an architecture implementation framework is used. The idea behind MDA is easy to grasp, but the implementation details are somewhat more elusive. Automated transformations, especially fully-automated transformations, from models into implementation artifacts is difficult, and developing completely platform-independent models of an application is also hard to do, since knowledge of available implementation technologies always informs and constrains architectures. MDA is much easier to employ in the context of DSSE, where a well-understood and constrained domain, as well as reference architectures and existing frameworks provide a much better-elaborated foundation.

## 16.4 End Matter

This chapter has attempted to provide high-level overviews of some of the most popular and well-known standards used in practice. One thing that is not evident from this chapter is the level of detail in which many of these standards are specified. Some of the standards themselves exceed the length of this book, and supplemental books (and, in some cases, book series) have been written to help people understand and apply these standards.

Size is not rarely a good way to assess the value of a standard, however. For example, it stands to reason that large, detailed standards provide an immense amount of guidance, and this is indeed often the case. However, what kind of guidance do they provide? Often, large standards remain underspecified: they give the user too much freedom or too many options, often in an attempt to broaden their appeal or applicability. Many of the largest and broadest standards (e.g., DoDAF, TOGAF) prescribe extensive

processes and checklists. These are often impossibly detailed—a project that attempted to satisfy every requirement or piece of advice in these standards would never get around to actually building a system. Furthermore, deciding whether a project or its architecture are correct and consistent is an exercise most often left up to the system developers, with little guidance from the standards.

When using a standard, a developer or organization must always keep in mind the costs and benefits of the standard. Looking for and exploiting network effects should be a priority of anyone employing a standard. Some standards exploit network effects better than others. For example, a standard like UML is well-supported by mature tools because of its large user community, and UML models can be used to more efficiently communicate ideas among different people and organizations because of common understanding of the meaning of different symbols. However, a process standard may have less network effect: the value of the process does not necessarily increase simply because more organizations use the process unless improved tool support or process refinements are a side-effect of that use.

The standards in this chapter document many “best practices”—well worn techniques that have been successfully used on projects in the past. Following any of these practices is undoubtedly better than a completely ad-hoc development, and the standards at least provide a yardstick against which completeness or comprehensiveness can be measured. Many important decisions, such as when enough modeling has been done, or what specific process to follow and how to define individual project goals, must still be made on a case-by-case basis. More specific and detailed guidance will not be found in the most generic (and unfortunately, well-known and well-supported) standards. Developers may have more luck combining the breadth of generic standards with more specific domain-specific standards—if such standards exist.

**Sidebar: The Business Case**

From a business perspective, standards can be seen as a “make-or-buy” decision. Adopting a standard confers many benefits: adopters are essentially buying the experience and time of previous engineering efforts, vendors, and so on. As those organizations evolve the standard, the quality of the standard ‘upgraded’ effectively for free, and organizations can make decisions on when and whether to move to the latest version of a standard.

Standards provide tremendous value by creating network effects: the more organizations that use the standard, the more valuable the standard becomes. If multiple organizations are involved in a single development effort, standards are often the best way to minimize communication

breakdowns and integration difficulties that can kill an otherwise successful project.

In keeping with the message of this chapter, the biggest business threat is getting overly invested or faithful in a particular approach when that faith is not warranted. The most reasonable approach is to adopt the standards that make sense, but prepare for a moderate investment in figuring out how to tailor those standards for your purposes. Many businesses and organizations adopt standards with the mistaken assumption that all their business problems will be addressed if they simply follow the standard to the letter. As we have attempted to convey in this chapter, many of the most well-known, well-supported and popular standards are often the most general and underspecified. Keeping a rational perspective on the scope of these standards is a must for any development organization. Organizations should define their business goals and the strategies for achieving them independent of any particular standard, and then choose and adapt standards that help them meet their goals based on these strategies.

## 16.5 Review Questions

1. What is a standard?
2. What is the difference between a *de facto* and *de jure* standard?
3. What is a network effect? How do standards help to create a network effect?
4. What are some drawbacks of standards?
5. What are the advantages and disadvantages of adopting a standard early? What are the advantages and disadvantages of adopting a standard late?
6. What is the scope of IEEE 1471? How does it advise and guide users?
7. Describe DoDAF. How does DoDAF help its users? What does DoDAF not provide?
8. What is TOGAF and how does it differ from DoDAF? What is the difference between enterprise architectures and software architectures, as they have been described in this book?
9. What are the five RM-ODP viewpoints? What kinds of systems is RM-ODP targeted for?
10. What are UML profiles and how do they help users in applying the UML standard?
11. What is SysML and how does it differ from UML?
12. What lessons can be learned from the standardization efforts behind ADML and AADL?

13. Enumerate some standard architecture tools. How do standard tools augment standard notations? How can they hinder the use of a standard notation?
14. Enumerate some process standards. How do process standards augment and interact with other standards?

## 16.6 Exercises

1. Obtain and read one of the standards listed in this chapter. Choose a system with which you are familiar (or one of the ones used as an example in this book, such as Lunar Lander or the World Wide Web) and outline how it would be described or implemented using that standard. Identify the standard's strengths and weaknesses in the context of your experience.
2. Draw out and discuss the relationships between the standards discussed in this chapter. Are they mutually exclusive? Do they dovetail with one another? Are they sequential? Identify some software development standards not discussed in this chapter and add them to your diagram.
3. Find an architectural model that claims to conform to one of the standards in this chapter. Check it for conformance against the standard itself.
4. Choose a standard and investigate how it is described and marketed by its creators and others. Assess whether the benefits (and drawbacks) claimed of the standard are accurate or not.
5. Contact one or more software development practitioners and find out about their use of standards. Ask what benefits they believe they are deriving from the use of the standard, and assess whether their development experiences have borne these out.
6. Find a tool-set that purports to support a particular standard. Select various elements of the standard and determine how they are supported by the tool-set. Identify how the tools help or hinder the use of the standard.

## 16.7 Further Reading

As with earlier chapters such as Chapter 6 on modeling, this chapter attempts to distill and extract the essence of some of the most well-known and influential standards in software engineering today. Still, the few pages dedicated to each standard cannot capture the scope of most of them. As noted above, the length of several of these standards exceeds the length of this book.

The best way to learn about a standard is often to go to the source. References are included below for IEEE 1471 [130], DoDAF [67], TOGAF [282], RM-ODP [136], UML [24] and its metamodel the MOF [211].

SysML [269], AADL [73], ADML [262], Rational Rose [237], Telelogic System Architect [279], RUP [159], MDA [199], and others. Beware the 'executive summaries' contained in some of these standards or related documentation; these descriptions are often heavy with hype and it is difficult to get a clear assessment of a standard from them. For comparative purposes, it might be useful to examine non-architecture-related standards such as POSIX [132] and HTTP [74] or domain-specific standards like the Software Communications Architecture (SCA) [195], introduced in Chapter 15.

## CHAPTER 17

**17 People, Roles, and Teams**

It has become quite common for a software engineer to be granted a title such as “software architect”, “senior software architect”, or “chief systems architect” in a software development organization. Such a title appears to carry with it a certain amount of prestige. The usual assumption is that the engineer in question has exhibited exceptional skills in software system design, familiarity with the modern development technologies, and/or ability to communicate a vision for a project, effectively interact with system customers and managers, and lead his fellow engineers in completing the project successfully. At the same time, if one looks a bit further, chances are that he will find many different descriptions of what the software architects actually do from one company to another, and even from one project to another within a single company. We find that in some companies “chief architects” are brilliant engineers who worked “in the trenches” for many years and emerged as technically savvy sages, while in other cases they are former CEOs who decide to step down and shift their focus to ensuring their company’s marketplace presence and setting the company’s long-term technical strategy. What this means is that, in fact, simply having the title does not mean one has the qualifications.

Clearly, this is very different from, say, an electrical engineer or even a software engineer: becoming one usually requires completing an appropriate four-year college degree at a minimum, and perhaps a further number of years of practical experience with specific additional training. By contrast, it is not all that unusual that a person with “software architect” in his title is not even a software engineer by training. This carries with it a significant danger: identifying, nurturing, and promoting a software architect becomes similar to building an underspecified software system. In software development this is sometimes referred to as the IKIWISI syndrome, or “I’ll know it when I see it”. Discovering the “right” software system, just like discovering a good software architect, under such conditions can be too time consuming, too risky, too unpredictable, and too expensive. Moreover it is also unclear how one can go about becoming an architect: the title tends to be bestowed upon, or sometimes assumed by, a person rather than earned through a well understood set of

steps. And should that person move to a different organization, or even a different division within the same organization, the same set of job responsibilities might carry a completely different title. Finally, with very few exceptions, one will not find a training program within a (future) development organization that helps an individual get that job or an appropriate title.

If our goal is to study software architecture as a mature discipline with well-understood and codified objectives, principles, and practices, then we must define the roles and responsibilities of the discipline’s practitioners, namely, software architects, more clearly. This chapter will do just that. We are guided by the observation that software engineering is a multi-faceted discipline which combines

- *core engineering skills* – for example, formal system modeling, code production, and product testing and measurement,
- *organizational skills* – for example, project management, cost estimation, and adherence to industrial and government standards, and
- *inter-personal skills* – for example, communication with many stakeholders, honoring one’s roles and obligations within a team, and putting the project’s success before one’s own personal goals.

Since software architecture permeates the entire software engineering process, and in many ways forms its core, it is not unreasonable to require that software architects possess a large cross-section of these skills.

The goal of this chapter is to answer four key questions:

1. Who are software architects?
2. What do software architects do?
3. How do they go about doing their job?
4. How do architects relate to, and interact with, other stakeholders in designing, implementing, and evolving a system’s architecture?

The first question deals with the core set of skills a software architect must possess, including both technical and non-technical skills. The second question sheds light on what a software architect’s job actually entails. The third question addresses how software architects are organized into teams, and how and when they move from one project to another. Finally, the last question takes a broader perspective on software architecture in practice as an exercise in consensus building in order to satisfy all of a system’s stakeholders. We will address each of these questions in more detail next.

## Outline of Chapter 17

17 People, Roles, and Teams  
17.1 Who Are Software Architects?

- 17.1.1 Architect as a Software Designer
- 17.1.2 Architect as a Domain Expert
- 17.1.3 Architect as a Software Technologist
- 17.1.4 Architect as a Standards Compliance Expert
- 17.1.5 Architect as a Software Engineering Economist
- 17.1.6 Some Bad Habits
- 17.2 What Do Software Architects Do?
  - 17.2.1 Develop Project Strategy
  - 17.2.2 Design Systems
  - 17.2.3 Communicate with Stakeholders
  - 17.2.4 Lead
- 17.3 How Do Software Architects Work?
  - 17.3.1 Balance of Skills
  - 17.3.2 Allegiance to the Project
  - 17.3.3 Allegiance to the Organization
  - 17.3.4 Duration of Involvement
  - 17.3.5 Team Structure
- 17.4 How Do Software Architects Relate to Other Stakeholders?
  - 17.4.1 Architects and Engineers
  - 17.4.2 Architects and Managers
  - 17.4.3 Other Stakeholders
- 17.5 Remaining Challenges
- 17.6 End Matter
- 17.7 Review Questions
- 17.8 Further Reading

## 17.1 Who Are Software Architects?

It has been said that software architecture is a result of applying “method, theft, and intuition” [156].

- *Method* refers to a well understood, codified set of steps that can be repeatedly executed to solve a particular problem, or category of problem.
- *Theft* refers to the reuse of solutions that have been shown successful in the past.
- *Intuition* is the ability to conceive, understand, and apply ideas without necessarily being able to communicate or explain the entire rationale behind them.

In fact, the reader has seen different elements of method and “theft” – that is, reuse – discussed throughout this book. These include reliance on effective techniques, processes, and existing solutions, such as styles, patterns, and entire DSSAs.

In many ways, the essence of a software architect’s job is to be able to apply and find the right balance among these three “sources” of architecture. In addition, by definition an architect is given a great deal of responsibility on a project: the project will succeed or fail depending on the employed architectural solutions. In many software development organizations that responsibility is not accompanied with specific authority. Instead, the architect is usually considered by the management as one of the engineers, or at best as “first among equals”. In order to do his job effectively, the architect must then find another way to exert influence and lead. He must possess and rely on a number of skills. An architect must be

1. a software designer,
2. a domain expert,
3. a technologist,
4. a standards compliance expert, and even
5. a software engineering economist.

We will discuss each of these roles in more detail in the remainder of this section.

### 17.1.1 Architect as a Software Designer

First and foremost, a software architect must be an excellent designer of software systems. He must be able to recognize, reuse, or invent effective design solutions and apply them appropriately. He must be familiar with the key architectural styles and patterns that underlie the discipline of software architecture. An architect may even have some patterns and/or styles that are part of his private arsenal of design tools, amassed over time, possibly as a result of work within a specific domain or application family. Conversely, an architect must also be able to recognize ineffective or suboptimal designs, inappropriate styles and/or patterns, and design decisions “with strings attached”.

In an ideal world, a good architect would always be able to provide rationale for all his decisions. However, we should also recognize that truly great architects – software or otherwise – often leave their mark when they depart from conventional wisdom, for example, when they are faced with an unprecedented problem, or when they realize that an existing problem can be solved in a better way. Their inspiration in such cases may be difficult to rationalize.

To be a great designer of software systems, a software architect must be a skilled software or systems engineer, with years of experience that is both rich and varied, good communication skills, and a keen sense of aesthetics.

A software architect must be an engineer because ultimately he is solving engineering problems. More specifically, he must have training as a

*software engineer* because software systems exhibit many properties not shared by other types of engineered systems.

A good architect must have extensive experience because he must strive for the most effective balance of method, theft, and intuition for the problem at hand. For example, if he is dealing with an unprecedented system, he might need to rely on intuition honed by working on many different types of problem over the years and apply generic methods, such as object-orientation. On the other hand, if he is dealing with a variation on a known problem, he will be able to leverage directly his experience, and apply both specific methods and reuse solutions from prior systems.

The architect must also be a good communicator since he must convince many other people of his vision for the system. This includes, for example, other engineers who will actually build the system, but may also include the managers, external project collaborators, project customers and users, the venture capitalists who may have invested in the company, and perhaps even the company's board of directors.

Finally, the architect must have a good appreciation for aesthetics. Those who cultivate such appreciation of design in the real world do a better job of designing in the software world. We will only briefly stress on this point here, but remind the reader of the discussion throughout the book (for example, see Chapters 1, 4, and 11). Elegant designs promote excitement about a project among its stakeholders, including the developers. They are remembered, studied, and emulated. In contrast, boring designs are not.

### 17.1.2 Architect as a Domain Expert

Many software development organizations produce multiple systems within the same application domain. For example, Microsoft works primarily within the domain of desktop applications; Google's primary domain of interest is information dissemination and use over the Internet; companies such Boeing and Lockheed Martin have an extensive focus on embedded systems; NASA produces ground-, Earth orbit-, and space-based systems.

In some cases, the domain of focus will be accompanied by one or more DSSAs (recall Chapter 15), which codify the characteristics of the problem being tackled as well as the solution developed in response. The burden of intimate familiarity with the application domain and the greatest risks of inappropriate and ineffective solutions are removed from the architects in such systems; they need only familiarize themselves with and stick to the prescription contained in the DSSA.

However, the systems being developed in some companies will only loosely be related, such that they cannot be consolidated into a DSSA. In those cases, each system will create its own challenges. The software architects working on such systems will need to have an intimate understanding of each application domain, its major properties, and its idiosyncrasies. Otherwise, regardless of their skills as designers, architects are likely to produce designs that do not work well for the type of task at hand. They may have problems communicating with other stakeholders, including other engineers. And they may not be able to use the properties of the domain to their advantage when facing a problem with their architecture.

### 17.1.3 Architect as a Software Technologist

A software architect must know that his solutions will actually work once fully developed. Just like a building architect needs to ensure that his designs can be constructed, so a software architect needs to ensure that the software technology exists to support his ideas. A beautiful design is useless if it cannot be implemented.

An architect's primary role, and likely even his main strength, is not as a programmer. Indeed, experience has shown that outstanding programmers do not necessarily make outstanding architects. At the same time, the architect cannot divorce himself completely from programming. The reasons behind this are analogous to the arguments made throughout this book for why it is unrealistic to isolate completely a system's architecture from its implementation. The architect must progressively elaborate design concepts into concrete elements. To do so, he may need to prototype specific elements of his solutions to ensure that they will behave in practice as envisioned. He may need to test out ideas on the exact execution platform on which the system will run. The architect may also need to convince either managers or developers that a particularly controversial idea is worth pursuing, by showcasing its benefits in practice.

Architects must also have a grasp of the generic capabilities software developers will have at their disposal when implementing the architecture. In the previous chapters we have covered many such technologies and shown that they can have a direct bearing on a system's architecture. This may include the details of the operating systems and programming languages on which the eventual application will run. It may also require the architect to familiarize himself with the latest advances in software libraries, frameworks, middleware platforms, networking solutions, and so forth. The architect's job is not only to ensure that his ideas can be implemented; it is to ensure that they can be implemented effectively and that the process of creating that implementation is efficient.

Additionally, the architect may need to play the technologist card because of perceptions. Due to the nature of the job, the architect must project authority with different stakeholders. Since an architect often is not a manager on whom authority is explicitly bestowed, that authority must be earned. This is especially the case in the architect's interactions with engineers who have no competence in software development, yet who may be the architect's most important clients. Engineers are typically highly educated and skilled themselves, very protective of their work, and may feel that they are capable of solving a particular problem just as well as the architect – regardless of their lack of any genuine qualifications in software. Being able to demonstrate technical prowess on occasion will help the architect remind the engineers that he is one of them, of the reasons he holds the job, and that he does not live in the proverbial ivory tower.

#### 17.1.4 Architect as a Standards Compliance Expert

As discussed in Chapter 16, many government, legal, and technical bodies produce standards to which a development organization must adhere. Some of those standards are mandated externally and are the pre-condition for bidding on contracts. For example, many projects funded by the U.S. Department of Defense must adhere to the C4ISR architectural framework. Other standards may be required by the company's management. For example, a company may decide to use UML 2 as an architecture documentation tool.

In either case, the software architects must be intimately familiar with the relevant standards. They must be able to accurately assess and communicate the value of specific standards, or the lack of appropriate standards. They must understand a given standard's expected impact on the architecture and on the eventual product – both positive and negative. They must be able to explain that impact to other stakeholders. Finally, they must be able to demonstrate that their architectural solutions adhere to any chosen standards, for example, in the case of a project audit.

The architect should also follow different standards efforts that get underway. A standards body may produce a technology that will significantly simplify development of future products, improve modeling and analysis capabilities for existing architectures, or ensure easy interoperability with important third-party software. For example, the emerging AADL architecture modeling notation which was discussed in Chapter 6 may provide modeling capabilities that UML does not possess; a given extension to the CORBA standard may ease system implementation; and so on. Additionally, actual participation in standardization efforts may help prevent ill-conceived and resource-wasting standards from being imposed on future projects and software architects.

#### Standards compliance roadblocks

Despite his best efforts, a software architect may at times be unable to ensure full compliance of a given architecture with a given standard. There are at least two possible reasons for this.

First, the standard may be loosely defined. It may provide a set of general guidelines, rather than a rigorously specified notation, technique, or process that an organization can follow and use. An example of a loosely defined standard is DoDARF, which was discussed in the preceding chapter. Another example is UML itself: while its syntax is precisely defined, its semantics is not.

The second reason a standard may be hard to comply with is that the tools built to support the standard in fact deviate from it. Thus, for example, a leading UML-based software modeling environment is IBM/Rational Rose. However, throughout UML's existence and evolution since the late 1990s, Rose has tended to deviate from the OMG standard, even if only in subtle ways. In such a situation, an organization that purchased Rose for modeling its software systems would be induced to deviate from standard UML.

Of course, the opposite of this argument also holds: these very reasons make it difficult to argue that an architecture does *not* comply with a standard.

#### 17.1.5 Architect as a Software Engineering Economist

A great software designer is not necessarily a great software architect. His designs may indeed be superior when looked at in isolation, but in the context of a particular organization or project, they may be unrealistic, overly expensive, technologically too ambitious, in violation of certain technological agreements or legal codes, or too risky for a multitude of other reasons. In other words, an architect must be more than just a (great) designer. An effective architect must produce an architecture that effectively addresses the problem at hand while simultaneously respecting the constraints placed on the project. If it fails on either count, that architecture will very likely result in a failed project.

One of the frequent constraints in real-world projects is money. Some companies competitively bid for contracts whose size constrains what can be done in the course of the project. Examples of such companies are large enterprises that work on government-funded projects in the United States and Europe: Lockheed Martin, Boeing, Marconi, and so on. Other companies get a finite, frequently quite small amount of venture capital to produce a successful system. Examples include many "dot.com" start-ups.

Yet other companies go to their own coffers to fund a project that is expected eventually to turn a profit. Such companies include large commercial software outfits, such as Microsoft, Yahoo, and Google.

In each case, when producing an architecture for a system under development, the architect must not only be aware of the monetary constraint, but must also be able to determine whether his solution can be effectively implemented within the project's budget. This means that the architect must have some, at least basic, understanding of the economics of software development, and must accompany his design decisions with, possibly quick and crude "back of the envelope" calculations of how much their implementation is likely to cost. Budgetary considerations may also lead the architect to opt for adopting or adapting existing architectures and for going with off-the-shelf functionality. Being able to provide appropriate economic justification for all such decisions is an integral part of the architect's job. Ultimately, the architect must also be constantly aware of the fact that the solution he produces may very well be technically sub-optimal.

### 17.1.6 Some Bad Habits

There are also certain tendencies an architect must avoid. Some obvious bad habits are discussed here; the reader may be able to identify others as well.

**Perfectionism.** The constraints inherent in the architect's job will often make it impossible to produce the perfect architecture for the given problem. Among the many reasons discussed throughout this text, at any given time the architect is likely to possess only partial information. That information may change over time such that, as the architect discovers new details about the system he is working on, previously held beliefs become invalid. Striving for perfection in such a fluid environment is impractical. In fact, one's ability to acknowledge, respond to, and even embrace change will be a mark of one's success as a software architect. This leads to the second bad habit.

**Inflexibility.** An architect should avoid insisting on a single correct or "best" way of constructing a system. A basic, positive, tendency of a designer should be to produce a clean and simple design. When constructing a building, bridge, or dam, this may mean clearing the building site so that the site fully reflects the architects' and engineers' vision. Unfortunately, it does not always work that way with software. Very few large systems are built from scratch, using a single architectural style, one's favorite set of patterns, standard middleware, programming language, operating system, and hardware platform. Instead, a software architect is much more likely to have to mix and even invent styles and patterns, look for new middleware platforms that solve the new problem

more effectively, address multi-lingual development on multiple platforms, and so on. The reasons for this may be legitimate technical considerations. The reasons may also be the many conflicting and changing requirements levied on the architecture and the architect by the other system stakeholders. In many ways a big element of a software architect's job is deciding whom to disappoint.

**Micromanagement.** Another bad habit for a software architect is the impulse to micromanage. An architect produces designs that may result in huge systems developed by many teams, possibly from many organizations, over a significant time period. Making sure that everything goes perfectly and that everyone adheres to the architect's vision at all points in time is simply not possible. It is also not the architect's job. A good architect will recognize that he is surrounded by highly skilled engineers and that many, or even most, of them will be able to do their own jobs much better than he will. Furthermore, trying to meddle in their jobs may create resentment and undermine the architect's goal of leading by example.

**Isolationism.** Finally, the architect should not isolate himself. Even though the architect may feel that the weight of a project is on his shoulders and that, at least early on in the project, he bears the greatest burden, the architect must remember that he is part of a much larger team, and that an integral part of his job is to ask, watch, listen, and communicate. The architect may get solutions to his specific problems in the process. He will also get the early buy-in from the stakeholders, a sense of joint ownership of the architecture, and set the stage for the architecture's eventual implementation. Shutting oneself in a room because one is "the architect" will likely achieve the exact opposite effect.

Another aspect of isolating oneself is insisting on always devising and using one's own solutions. Even though at times there may be a legitimate need for an architect to invent new design techniques, notations, patterns, or styles, the accompanying danger is doing this even when it is not necessary. This is often referred to as the "not invented here" syndrome: architects and, more broadly, organizations are sometimes unaware of, or even deliberately ignore, known effective solutions and insist on developing their own instead. Closely related to this is the "we have always done it this way" syndrome, where suboptimal or even ineffective solutions are applied repeatedly because they may have been demonstrated to nominally work in the past (possibly in very different contexts and on very different problems). Both of these situations are risky, expensive, and frequently result in duplicating the work someone else has already done or, worse, producing inferior solutions.

**The Ultimate Bad Habit**

In many software development organizations, especially startups, the chief architect is the person who came up with the original idea upon which the company was founded. That person may hold other titles and responsibilities in such an organization, such as Chief Technical Officer or even Chief Executive Officer. Alternatively, a new owner of an existing company may assume the role of the chief architect of the company's flagship product or its entire line of products.

The responsibility placed on such individuals is clearly greater than it is on "mere" architects: they are responsible for much more than just the technical success of a product. At the same time, these individuals' prior successes, especially if they were big successes—think, for example, Netscape—can become an impediment to doing smart business (and smart architecture). The relatively brief history of the software marketplace teaches us that the fortunes of a product, and of a company, can change rapidly. Therefore, delusions of grandeur are the ultimate bad habit for software architects.

In his fun, insightful, and sobering book "In Search of Stupidity"[37], Merrill R. (Rick) Chapman chronicles several examples of this ultimate bad habit of software architects from the past couple of decades. He explains how and why certain companies—including aforementioned Netscape—have gone from a market leader to a historical footnote through an often rapid succession of missteps, both managerial and architectural. Chapman's book serves as a useful reminder of the need for careful planning, good software architecture, solid engineering practices, and, above all, humility.

## 17.2 What Do Software Architects Do?

By now it should be clear that a software architect's job will require showcasing a number of diverse skills. Being an effective designer is one such skill. However, an architect will spend much of his time doing other things. We will briefly discuss four tasks an architect will most likely have to perform regardless of the type of project, his level of experience, the organization for which he is working, the application domain, the industry segment, and so on. In accomplishing these tasks, the architect will repeatedly have to apply, combine, and extend the skill set described in the preceding section.

### 17.2.1 Develop Project Strategy

A talented software designer will most often be able to produce an excellent technical solution for the problem at hand. That solution, however, may not be the best one for the *project* or the *organization*

solving the problem. A talented software *architect* will have to recognize the distinction between the two, and make sure always to address the latter. The architect's primary job is to help develop a comprehensive strategy for the project. That strategy, if appropriately implemented, will not only result in a system that is a good technical solution, but one that also becomes a valuable product for the organization.

This requires understanding the economic context of the project and the organization, the competition in the marketplace, and any standards and regulations by which the organization must abide. Perhaps most importantly, the architect must be intimately familiar with the human as well as technical resources at the project's disposal. An otherwise outstanding design will have a high likelihood of failure if it requires purchasing a lot of expensive new technology, retraining the existing engineers, or hiring many new staff.

### 17.2.2 Design Systems

A central part of overall project strategy is design of the system's architecture. Once an architect is aware of all the relevant constraints being faced, he is ready to proceed with solving the problem. This is likely to be the most enjoyable part of architect's job. Paradoxically, it may also be the most stressful.

An architect will likely enjoy designing systems because he will get the opportunity to design, use his imagination and creativity, put his stamp on the future systems, and perhaps even to think outside the proverbial box. However, the architect will still need to be in frequent contact with other stakeholders, gather information from them, and respond to their possibly conflicting requests. He will have to deal with the likelihood that he may not have the complete picture at his disposal, and that that picture is constantly changing. It has been said that the job of a software architect is a succession of suboptimal decisions made in semi-darkness. The architect will also have to avoid letting personal goals, such as producing a "clean" design in record time, override the other stakeholders' concerns.

### 17.2.3 Communicate with Stakeholders

Throughout the process of developing the project strategy and producing the architectural design, the architect will have to be in frequent contact with the system's different stakeholders. One of the main factors in the project's success is whether the architect can project and ensure a continued, coherent vision for the resulting system. In that sense, his job has something in common with a salesman, with the added caveat that he is negotiating with and "selling" the project to many different types of customers in many different ways: developers, testers, technical leads, managers at all levels, customers, users, and so on. The architect may need

to do so repeatedly, especially in a long-lived project, where the overall vision may be temporarily lost in the details. In such situations, the architect may also need to assume the role of the project's "cheerleader", maintaining the morale of the different stakeholders. He may also need to show significant awareness and political savvy regarding the competing interests of the various stakeholders in order to carry out this task effectively, remembering throughout that being an architect often involves having to decide whom to disappoint.

While the architect may be using different languages to communicate with the different stakeholders, and may focus on different aspects of the project depending on the situation, throughout this process he must ensure the architectural integrity of the project. The compromises the architect will inevitably make cannot be allowed to undermine the overall objective, or to clash with other decisions he has previously made for reasons that are just as valid. Throughout this process he must strive to avoid architectural degradation.

#### 17.2.4 Lead

An architect will make many decisions that are crucial to the project's success and will have to convince a broad audience, a part of which may be skeptical, that those are correct decisions. Some of those decisions may be unpopular, yet the architect will need to get the buy-in from all the major stakeholders, and must do so continuously throughout the project's life span. In some situations, just getting buy-in may not be good enough; the architect may need to elicit excitement for the project. He will frequently have to assume this responsibility without any explicit authority over the stakeholders with whom he is interacting.

To do so, the architect will have to be a leader. While it may be difficult to teach, leadership is a skill that can be nourished and refined. To be an effective leader, an architect must

1. show confidence in the project's success,
2. project conviction in his ideas,
3. demonstrate readiness to assume full responsibility for any technical problems,
4. be ready to articulate the technical rationale for design decisions,
5. be able to further develop the project's detailed architecture,
6. acknowledge contributions of others, and
7. avoid self-aggrandizement.

At all times, the architect must put the interests of the project before his own, and lead by example. Developing a complex software-intensive system may require sacrifices from engineers, including long hours, working weekends and holidays, and time away from families. An

architect who is a true leader will always be prepared to make his share of the sacrifices. He must also know when making such sacrifices are inappropriate, and should ensure that project personnel are treated with respect and consideration.

### 17.3 How Do Software Architects Work?

An architect may work alone or, more likely, as part of a team. The exact composition of an architecture team and its precise role during the various project stages may vary from one organization to another, and even from one project to another. However, teams should be built with certain generally applicable guidelines and observations in mind, as discussed below.

#### 17.3.1 Balance of Skills

The software architecture team must be composed from people whose strengths are complementary and cover the range of skills discussed above. It is unlikely that a single person will be an outstanding designer, domain expert, technologist, communicator, *and* leader. More likely, each architect's primary strengths will be in a small number – perhaps only one – of these areas.

Composing the architecture team from people with similar skill sets will thus clearly not be helpful. For one, certain project needs, such as design, may be overstuffed, with a danger that the architects will get in each other's way, while other aspects of the architecture, such as domain expertise, may suffer. At the other extreme, staffing the team with architects whose skills do not sufficiently overlap carries the danger that the information gathered and architectural decisions made will neither be properly understood by different team members nor integrated into a coherent whole.

The architecture team will carry a great deal of responsibility for and exert dominant influence on a project. Thus, it must be staffed with qualified people. Kruchten makes the interesting observation that the architecture team should not become a "retirement home" for ageing software engineers [157]. This may seem like an unnecessary admonition. However, it is not all that uncommon that engineers with outdated technical skills in large organizations are simply "promoted" to software architects. This is seen as the easiest way of minimizing the negative impact of such engineers' deteriorated abilities. This can be very dangerous and, simply put, it is patently stupid.

#### The Peter Principle

A failure by an organization to staff its software architecture team with competent people can be viewed through the prism of *The Peter Principle*.

This principle was formulated by Laurence J. Peter in his 1969 book of the same name [222], and states that “In a hierarchy every employee tends to rise to his level of incompetence.” In other words, a member of a hierarchical organization is eventually promoted to his highest level of competence; any subsequent promotion will elevate the employee to a position for which he is no longer competent, i.e., to his “level of incompetence”. Once he reaches his level of incompetence, the employee’s chances of further promotion are low. However, from a practical perspective, by that time the damage may already have been done.

For example, an excellent C programmer within an organization may receive many salary raises, and may progress through the company’s hierarchy of software engineering positions: “software programmer”, “software engineer”, “senior software engineer”, “principal scientist”, and so on. At some point, for reasons discussed in this chapter, this employee may be promoted to a position of “software architect”, for which he may be poorly qualified. Such a position is likely too important and carries too much responsibility for the organization to be able to afford letting this employee take the time to learn his new job. However, the organization may have no other choice, unless it wants to demote its otherwise excellent engineer. In the meantime, the likelihood of failed projects will be elevated.

The dire implication of the Peter Principle is that an organization is prone to collapse if a sufficient number of its employees reach their levels of incompetence.

### 17.3.2 Allegiance to the Project

The software architecture team should be an integral part of the project, and should be associated with the project throughout its lifecycle. Both the architecture team and the other stakeholders must understand that the architecture team is invested in the success of the project. To the architects this is important because of the architecture team’s need to exert influence over all principal design decisions whenever required. To the programmers it is important because they must feel that the software architects are “one of us”. To the managers and customers it is important because they can clearly see accountability for the architectural decisions made.

An alternative to this view is to treat the software architecture team as a consulting entity that jumps in depending on the needs of different projects. This can be dangerous for several reasons. If a project

experiences difficulties, such a setup may introduce an “us versus them” division. Furthermore, the implicit lack of accountability and oversight by management in that case makes it less likely to get buy-in from the stakeholders: for example, if developers believe that it is their responsibility alone to build a successful system and that the architecture team is a marginally interested third party, they will be less likely to take and implement the architecture team’s advice, thus possibly violating critical architectural decisions. Most importantly, it is highly unlikely that a part time software architecture team can simply show up whenever needed, understand all the nuances of the system, make appropriate decisions, and move on.

We should recognize the tension that will inevitably appear between the need of the project—to have a readily available software architecture team—and the need of the organization—to leverage the most experienced, talented, and effective architects across multiple projects that may be undertaken simultaneously. There is no easy solution to this problem, and different organizations may try to address it in different ways. For example, more experienced, senior architects may move to another project once a given system’s architecture is reasonably stable, while the junior architects would remain with the project, assume additional responsibilities, and further hone their skills.

### 17.3.3 Allegiance to the Organization

If one Googles the phrase “software architect”, one will find a number of Web sites belonging to consulting firms. These firms specialize in providing software architecture “services” to other software development firms. Their mode of operation is to come into an organization, familiarize themselves with the project and possibly the problem domain, and help develop the appropriate architecture for the system under development. At first blush, this may seem like the part time software architecture team pitfall mentioned above. However, these teams may be hired to staff the project throughout its duration, alleviating that particular concern.

The real question in this case becomes whether it is preferable to employ a permanent software architecture team that will be part of, and thus fully accountable to, the software development organization, or to outsource this important, but possibly scarce and expensive, capability. The conventional wisdom would suggest that having a native software architecture team is preferable. That stance is probably influenced by the traditional view of software development in which an organization owns a project and develops it in-house completely. Such organizations and projects still exist in some cases, an obvious example being Microsoft, and this view may be appropriate for them.

The answer to the question of whether to employ or hire a software architecture team becomes more complex in the case of many other development organizations. The reasons are two-fold. First, a typical software project will use a number of off-the-shelf technologies and even application-level components. In such situations, the question becomes, who actually owns and controls the software architecture? It has been shown that such technologies directly impact a system's architecture [61]. Therefore, by importing an off-the-shelf capability, one, at least in part, imports an architecture as well, and the perception may be that there is less of a need for an in-house architecture team. This may indeed be the case in certain situations. But beware: the danger in such an argument is that by letting a chosen third-party technology control one's architecture, one is in fact relinquishing a critical piece of control over the project to someone who

- did not have that project in mind when they developed their technology,
- may not have taken into account, or even been familiar with, any aspects of the problem domain, and
- is unfamiliar with the organization, the skills of its engineers, the technical and economic context of the project being undertaken, and so on.

In effect, doing this is akin to letting the tail wag the dog.

The second consideration in deciding whether to maintain an internal architecture team has to do with the software development model that has gained increased popularity: outsourcing. Usually a development organization will find it economically advantageous to hire outside developers, often in a foreign country, to implement parts of a system. It might be argued that, by extension, the architecture of the system can be outsourced as well. On the surface, this is similar to hiring an external architecture team. However, relying on the external architecture team assumes that the team would still need to understand the details of the project and its requirements, work in close collaboration with the other system stakeholders, get their buy-in, and oversee the architecture's implementation and evolution. Simply purchasing a putative architecture for a project from a third party is usually not feasible, unless the organization is branching out into a new business area having a well-established existing architecture.

One potentially positive aspect of hiring an external software architecture team or outright outsourcing of the architecture is that it might be an effective way of avoiding both the "not invented here" and the "we have always done it this way" bad habits discussed above. Even here, however, this risk can never be completely eliminated: the "here" and the "we" may just be shifted to the external team.

### 17.3.4 Duration of Involvement

The software team does not disband and/or disassociate itself with the project after the architectural design activity is over. There might be an impulse to do so since the team's task is considered to have been completed, and other projects may need architectural help. However, moving the team to other projects will have a similar effect to that of treating the team as a consulting entity. More importantly, we have stressed several times throughout this book that it is inappropriate to think of software architecture as a "phase" that is completed early on in a project. While most of the major architectural decisions may be undertaken during the project's early stages, the architecture remains an active, almost organic underpinning for the project that constantly changes and evolves. Cutting off the architecture team from the project will thus result in many critical architectural decisions that are made haphazardly, understood partially at best, and documented poorly if at all.

Instead, the architecture team must be closely involved with the project throughout the project's lifecycle. Once the architecture becomes reasonably stable, it may in fact be possible, and even advisable, to reassess some members of the architecture team to other projects. However, at least a part of the architecture team should remain on the project. In certain cases, members of the architecture team may be assigned as liaisons to the development teams. In other cases, they may become leads of different development teams. This will allow for the architecture team to have direct oversight of the project's progress, any difficulties encountered, adherence to the architecture, needed changes to it, and so on. It will also help reinforce the fact that the architecture team's primary allegiance is to the project, thus helping to improve the morale.

### 17.3.5 Team Structure

Software architect teams can be structured in different ways. This depends on the size of the software development organization, the number and types of projects on which the organization is working concurrently, and the organization's own management structure. We will briefly discuss three primary ways of structuring an architect team. Variations on these models are possible.

#### *Flat Model*

The flat model usually works well in small organizations. Architects in it are not stratified in any way, and carry comparable clout and responsibility. It is an egalitarian organization that comports well with mature professionals. On the other hand, with less mature or responsible individuals this organization may cause problems in cases of disagreements, whether within the architect team or with other

stakeholders. It may also overwhelm the architects because of the unspecified or inadequate division of responsibilities. This model may not scale well to large teams and large projects. An extreme case of a flat architect model is that of a single software architect working on a project.

#### *Hierarchical Model*

A much more practical model, especially in larger organizations is the hierarchical model. This model was identified as early as Fred Brooks's *Mythical Man Month* book [31]. In this model, the architect team is typically headed by a *chief architect* or *senior architect*, and staffed with *junior architects*. In some, typically large organizations the architect team may be further stratified. For example, an *enterprise architect* may be in charge of the software architectures of all of that organization's different projects. The division of responsibilities and authority in the hierarchical model is clearly defined. This makes it more easily scalable to large teams. The potential downside is that the architect team must in effect assume an internal management structure, in addition to and separate from that in the rest of the organization.

#### *Matrix Model*

In the matrix model, architects simultaneously work on multiple projects. A cross-section of skills is applied to a cross-section of projects. A single project may have multiple, changing architecture teams during its lifespan, depending on the expertise needed. This model can be found in organizations that are understaffed (perhaps unexpectedly), or experience periodic spikes in undertaken, externally funded projects. The matrix model is orthogonal to both the flat and hierarchical models: architect teams may, but need not be stratified. The main advantage of this model is that it is very flexible. However, this should be looked on as a temporary solution. It carries the danger that architects will be oversubscribed and constantly distracted by the many simultaneous problems on which they are working, and will be unable to devote appropriate attention to any of the projects.

## 17.4 How Do Software Architects Relate to Other Stakeholders?

It should be clear by now that a software architect exists neither outside nor above his organization. Instead, an architect is an integral part of a software development team, project, and organization. The job of an architect carries with it many responsibilities. In order to fulfill those responsibilities, the architect is forced to delegate and rely on his co-workers; communicate with and garner support from his managers; and keep customers and users in the loop as necessary. In this section, we will

outline the nature of these relationships, and the likely challenges an architect will encounter in maintaining them.

### 17.4.1 Architects and Engineers

A large project will typically have a number of engineering teams working on it. Different teams may be tasked with different facets of the system, and may include specialists in specific software engineering sub-disciplines such as requirements, quality assurance, implementation, and cross-application middleware.

The architect must have a close, well functioning relationship with all engineers. In the case of some, such as requirements engineers, that relationship may be more natural and objectives more mutually aligned than in the case of others, such as software testers. In either case, however, the guiding concern must be the overall success of the project.

Perhaps the most important constituency within the organization to the architect are the programmers. Programmers will realize and refine the architect's vision. They also serve as validators of the architecture: if an architectural design decision has unforeseen consequences, a programmer will likely be the first one to notice. In such cases especially, a close, cooperative relationship between architects and programmers is critical; if it is lacking, architectural degradation will quickly occur.

In many companies architects also must work closely with systems engineers and, in some projects such as embedded systems projects, hardware engineers. An architect's relationship with these engineers will likely be different than in the case of software engineers. One reason is that a software architect creates the overall vision and design for the *software* portion of the given system, but does not have analogous control over the remainder of the system. Another reason is that, since systems and hardware engineers lack training in software engineering, they may not have appropriate appreciation for the nuances of the system's software architectural design, and may fall victim to the misconception that, since software is infinitely malleable in principle, it should always change to accommodate the needs of other system components. By now the reader should be able to appreciate the fact that frequent changes to a system, especially if undertaken hastily, will tend to invalidate the key architectural design decisions, and result in architectural degradation.

A related, and even bigger, issue that may occur in the relationship between a software architect and non-software engineers is the lack of respect for the architect's importance to the project. This can, of course, happen with software engineers as well. All engineers working on a given project may be highly capable and may qualify as experts in their own focus area, whether systems, hardware, or some particular specialty topic.

They may thus feel that they understand the nuances of their task much better than the software architect does. Furthermore, they may not see the direct benefit of strictly adhering to the architecture; they are frequently more interested in achieving local optima due to their limited vision of the entire project. As already mentioned, in some development organizations software architecture, and software *architects*, are still not held in very high regard. Coupled with a dislike of being told what to do, this can result in significant resistance to the software architect and hence contribute to a failed project.

Avoiding, or identifying and remedying such situations, is one of the main challenges and primary duties of a software architect.

#### 17.4.2 Architects and Managers

At times, an architect must achieve his objectives in the face of skeptical and even uncooperative engineers, and often must do so without any formal authority over those engineers. As discussed previously, the architect may have to resort to winning them over with personal competence and leadership. Clearly, things are likely to go more smoothly if he also has the support of the organization's management.

Software development organizations are increasingly beginning to understand the importance of software architectures and software architects. Management must work to ensure a project's success, and in an ideal world that would mean ensuring that the system's architecture, that is, the architects' vision, is realized fully and effectively. In turn, this requires architects and managers to interact frequently and to closely align their goals. This may mean that the managers must adjust their expectations of a project based on the architects' technical considerations. It may also require architects to adjust their expectations, and the architecture itself, based on the organization's realities: schedule and budget constraints, marketplace considerations, personnel turnover, and so forth.

Managers and architects do not always work well together, however. There may be many reasons for this, but from a software architect's perspective one reason can be particularly damaging: understanding the importance of the architect's role in a project does not ensure managerial competence. A project, and an entire organization, may be mismanaged in many ways and for many reasons. The managers also may simply lack the technical know-how to grasp the importance of the architect's design decisions. As a result, while a manager may in principle support the *architect*, he may unwittingly undermine the *architecture*.

Managers may fail to think through all of the consequences of their actions, which may negatively impact the system's architecture. They may

commit to purchasing and using third-party components, frameworks, or middleware that are a poor fit for the architecture. They may decide to comply with standards that cannot be easily "shoe-horned" into the company's existing architectures. They may also commit to delivering too much, too quickly, too cheaply, without understanding the architectural implications of those promises. These are challenges of which an architect must always be aware and may be forced to respond to.

Of course, an even bigger challenge faced by architects is in more traditional software development shops, in which certain techniques, tools, and processes may have ossified over time. In some parts of such organizations, architecture-centric development on the whole may be considered to be a fad, too inefficient, and unnecessary. Likewise, a particular architectural approach—for example, requiring that a developer request a formal architectural design review before he may change a component's interface—may go against the organization's culture, which in the past has relied on, and thus still encourages, a swaggering form of individual initiative. In such situations, architects must simultaneously fight two battles: arriving at an effective architecture for the system under construction, while at the same time trying to overcome institutional resistance, ignorance, and hubris.

#### 17.4.3 Other Stakeholders

Software architects must also interact with additional stakeholders, both within and outside their organization. Of particular importance is their relationship with the marketing department. In many organizations, innovation is frequently driven by market needs and pressures. This is, of course, understandable since a company's primary goal is to sell products. There is nothing inherently wrong or inverted in such an arrangement: the marketing department will research the current marketplace conditions and customers' needs, and will report those to the company's management or engineers; in turn, the software architects will employ their skills to design systems that will best take advantage of the market conditions and satisfy customer needs. It is, therefore, not unusual for marketing to drive a product's development, and hence its architecture: it may determine the systems that need to be built, their exact features, development priorities, release dates, and so forth.

At the same time, one must beware of certain pitfalls in this relationship. Both the architects and marketing staff may fail to properly understand the motivations, abilities, and expertise of the other. The architects may resist being told what to do, especially if they fail to appreciate that market conditions will occasionally get in the way of producing the best or preserving the originally envisaged architecture for a system. For example, an architect's task will be directly impacted if a potential competitor has been identified and it becomes imperative to release a product much

earlier than originally planned. So too if the primary customer base for the system under construction is observed to be moving to a different computing platform, or if the envisioned customer base expands or shrinks significantly. Architects will have no choice but to accommodate such non-technical realities.

On the other hand, the marketing department may cause problems if it fails to understand that a system's architecture cannot be arbitrarily or abruptly modified to incorporate newly identified needs. Marketing may also strive for unrealistic goals and unreasonable deadlines, and may attempt to drive the engineering process without adequate understanding of technical challenges and realities. In the most extreme case, marketing may promise a product that simply cannot be built by the company's engineers at the given time.

In either case, misunderstandings and lack of proper communication between architecture and marketing teams may result in an adversarial, counter-productive relationship between them. Keeping this relationship healthy should be an important, regular objective.

Somewhat similar to the architect's relationship with the marketing staff will be his relationship with the system's customers and users. The architect may need to interface directly with customers and users. In fact, he may well be the face of the project as far as the customers and users are concerned: the architect may present the project vision to them, ensure that their requirements are properly reflected in the system's blueprint and eventually in the system itself, address their inquiries, and resolve their concerns and doubts.

If properly established and nurtured, this can be a very productive relationship, whereby the system's final acceptance is ensured along the way, with all of the major issues addressed as they came up during construction. On the other hand, the customers and users may be very particular in their requests, impatient, and in the worst case insufficiently knowledgeable of the nature of software and nuances of its development. Thus, in addition to providing the rationale behind the architecture to the stakeholders within the organization (developers, testers, managers), the architect may also need to tailor that rationale for the benefit of the technically much less savvy customers and users.

## 17.5 Remaining Challenges

As the discussion above suggests, the architect must possess many skills, from maintaining the system's conceptual integrity to serving as the project's cheerleader, leading by the strength of technical knowledge and character, and interacting effectively with a broad range of stakeholders with frequently competing goals. While some of these skills cannot be

taught, they certainly can be nurtured. At the same time, there are several other facets of an architect's job for which he can be trained in a conventional manner—an observation that has motivated this textbook as well.

The principal challenge for software development organizations—including, but not restricted to, the traditional software shops that want to introduce software architects and explicit architecture-based software development for the first time—is identifying the best candidates for the software architect position, the appropriate skill set they should possess, and the people who can train them. There are several examples in industry of such training programs. One example is NASA Jet Propulsion Laboratory's Software Architect Program[300]. Such programs are relatively recent, and their effectiveness, and required adjustments, will need to be monitored over time.

## 17.6 End Matter

A software architect has a multi-faceted job, teeming with unique challenges and substantial responsibility. An architect may work alone or, more likely, as part of a team. His job description may be somewhat imprecise. It will involve many technical skills the reader has honed with the help of this book: architecture modeling and analysis; awareness of and proficiency with architectural styles and patterns; familiarity with product lines and domain-specific architectures; understanding of relevant implementation, deployment, and evolution technologies; and so on. One's job as a software architect will also require many skills that, at first blush, may not seem like those of a software practitioner, or that may not be readily learned from a book: the ability to communicate effectively with many different types of stakeholder; to ensure compliance with relevant laws, regulations, and standards; to lead; to ensure the architecture's economic viability. As an architect, one thus truly has to be a jack-of-all-trades.

### The Business Case

A critical success factor for a software system is that system's architecture. The skills of the architects and composition of the architecture teams will therefore have a direct and significant impact on the success of a project and of an organization. Each individual architect must be a jack-of-many-trades, while the architecture teams must have a comprehensive balance of skills.

Fred Brooks has opined that great designers must be spotted, selected, and nurtured. However, as we have seen, an architect's job is not restricted to design. He must possess a broad cross-section of skills. Many of those skills can be learned; all can be improved with study and practice. It is

thus in a company's interest to provide the appropriate training for its architects. It is also important to strive to achieve a careful balance in the architecture teams.

The bottom line is that a company with skilled architects and carefully composed architecture teams will have a better opportunity to succeed in the marketplace.

## 17.7 Review Questions

1. What are the necessary skills a software architect should possess?
2. What are some additional useful skills?
3. This chapter discussed several bad habits a software architect may exhibit. Can you identify any others? Be sure to justify your answers.
4. Your organization has identified an exceptional young software designer and would like to promote him into a software architect. What, if any, additional training would be required to accomplish this? How would you suggest that your organization proceed?
5. Based on the discussion provided in this chapter, present an argument why purchasing an architecture can be a recipe for failure.
6. Outsourcing software development has proven to be a successful strategy for many organizations. Should organizations also outsource architectural design? Be sure to carefully state your argument.

## 17.8 Further Reading

Brooks was one of the first to recognize the importance of a chief designer in a software project in his seminal book "The Mythical Man Month" [31]. Many of his observations, drawn from the experience of building the IBM 360 operating system in the 1960s, still ring very true several decades later and inspired several of the points in this chapter. Brooks followed that with an essay arguing for the importance of software design, and of great software designers, in tackling the essential difficulties of software engineering [30]. The dangers of the Peter Principle—which, as this chapter has argued, has a direct relevance to software organizations and architects— are described in Peter's book of the same name[222].

More recently, a number of authors have tried to answer the questions of who software architects are, what skills they must possess, and how they go about devising a system's architecture. Several of these issues were considered, at least indirectly, by Curtis, Krasner, and Iscoe [48] in the context of designing large-scale software systems, and then more directly by Kruchten [156, 157]. Kruchten's 1999 paper in particular provides an excellent elaboration of the desired skills and responsibilities of software

architects. A number of insights from that paper have found their way into this chapter. Several similar observations have also been made by other authors, e.g., Smolander [260] and Paivarinta[261]

DiNitto and Rosenblum's [61] provide one of many examples of the manner and extent to which technological solutions (in their case, middleware) impact a software system's architecture, and thereby the system's architects. Tracz's work on domain-specific software architectures (DSSA)[274, 288, 290]argues for the other critical facet of an architect's job – domain expertise.

In practice, as argued in this chapter, an effective software architect must possess many additional skills. A number of organizations have established software architect training programs with the objective of molding their architects into well rounded, multi-faceted employees. One representative example is NASA Jet Propulsion Laboratory's Software Architect Program [300].

## CHAPTER 18

**18 End Matter****18.1 Bibliography**

- [1] Telelogic DOORS. <<http://www.telelogic.com/products/doors/doors/index.cfm>>.
- [2] Argo/UML. <<http://argouml.tigris.org/>>.
- [3] Oxford English Dictionary. In *OED Online* Oxford University Press, 2007. <<http://www.oed.com>>.
- [4] Abbott, R.J. Program Design by Informal English Descriptions. *Communications of the ACM*. 26(11), p. 882-894, 1983.
- [5] Abdul-Rahman, A. and Hailes, S. Supporting Trust in Virtual Communities. In *Proceedings of the Hawaii International Conference on System Sciences*. Maui, Hawaii, Jan 4-7, 2000.
- [6] Albin, S.T. *The Art of Software Architecture: Design Methods and Techniques*. 312 pgs., Wiley Publishing, Inc., 2003.
- [7] Alexander, C., Ishikawa, S., and Silverstein, M. *A Pattern Language: Towns, Buildings, Construction*. 1216 pgs., Oxford University Press, USA, 1977.
- [8] Alexander, C. *The Timeless Way of Building*. Oxford University Press: New York, 1979.
- [9] Allen, R. *A Formal Approach to Software Architecture*. Ph.D. Thesis. Carnegie Mellon University, p. 248, 1997. <<http://reports-archive.adm.cs.cmu.edu/anon/1997/CMU-CS-97-144.pdf>>.
- [10] Allen, R. and Garlan, D. A Formal Basis for Architectural Connection. *ACM Transactions on Software Engineering and Methodology (TOSEM)*. 6(3), p. 213-249, July, 1997.
- [11] Apache Software Foundation. *Apache Derby*. <<http://db.apache.org/derby/>>, Website.
- [12] Atria Software. *ClearCase Concepts Manual*. Report, 1992.
- [13] Balek, D. and Plasil, F. Software Connectors and Their Role in Component Deployment. In *Proceedings of the DAIS '01*. Kluwer. Krakow, 2001.
- [14] Baset, S.A. and Schulzrinne, H. *An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol*. Columbia University, Report CUCS-039-04, 2004.

- [15] Bastarrica, M., Shvartsman, A., and Demurjian, S. A Binary Integer Programming Model for Optimal Object Distribution. In *Proceedings of the Second International Conference on Principles of Distributed Systems*. p. 211-226, Hermes. Amiens, France, December 1998, 1998.
- [16] Batory, D., Coglianese, L., Shafer, S., and Tracz, W. The ADAGE Avionics Reference Architecture. In *Proceedings of the AIAA Computing in Aerospace-10 Conference*. March, 1995.
- [17] Batory, D., McAllester, D., Coglianese, L., and Tracz, W. Domain modeling in engineering computer-based systems. In *Proceedings of the 1995 Internal Symposium and Workshop on Systems Engineering of Computer Based Systems*. p. 19-26, March, 1995.
- [18] Berners-Lee, T., Cailliau, R., Luotonen, A., Nielsen, H.F., and Secret, A. The World-Wide Web. *Communications of the ACM*. 37(8), p. 76-82, August, 1994.
- [19] Binns, P., Englehart, M., Jackson, M., and Vestal, S. Domain-Specific Software Architectures for Guidance, Navigation and Control. *International Journal of Software Engineering and Knowledge Engineering*. 6(2), p. 201-227, June, 1996.
- [20] Bishop, M. *Computer Security: Art and Science*. Addison-Wesley, 2003.
- [21] Boehm, B.W. A Spiral Model of Software Development and Enhancement. *IEEE Computer*. 21(5), p. 61-72, May, 1988.
- [22] Booch, G. Object-Oriented Development. *IEEE Transactions on Software Engineering*. 12(2), p. 211-221, 1986.
- [23] Booch, G., Rumbaugh, J., and Jacobson, I. *The Unified Modeling Language User Guide*. Object Technology Series. Addison Wesley Professional: Reading, Massachusetts, 1998.
- [24] Booch, G., Rumbaugh, J., and Jacobson, I. *The Unified Modeling Language User Guide*. 2nd ed. Addison-Wesley Object Technology Series. Reading, Massachusetts: Addison-Wesley Professional, 2005.
- [25] Bosch, J. *Design and Use of Software Architectures: Adopting and Evolving a Product-Line Approach*. ACM Press, Addison-Wesley Professional: Reading, Massachusetts, 2000.
- [26] Bowman, I.T., Holt, R.C., and Brewster, N.V. Linux as a Case Study: Its Extracted Software Architecture. In *Proceedings of the 21st International Conference on Software Engineering (ICSE'99)*. Los Angeles, CA, May 16-22, 1999.
- [27] Brand, S. *How Buildings Learn: What Happens After they're Built*. Penguin Books, 1994.
- [28] Bray, T., Paoli, J., and Sperberg-McQueen, C.M. *Extensible Markup Language (XML): Part I. Syntax*. World Wide Web Consortium, Recommendation Report, February, 1998. <<http://www.w3.org/TR/1998/REC-xml>>.
- [29] Briand, L.C. and Wolf, A.L. eds. *Future of Software Engineering (FoSE 2007)*. 379 pgs., IEEE Computer Society: Minneapolis, Minnesota, 2007.
- [30] Brooks, F.P. No Silver Bullet: Essence and Accidents of Software Engineering. *IEEE Computer*. April, 1987.
- [31] Brooks, F.P. *The Mythical Man-Month: Essays on Software Engineering*. 2 ed. 336 pgs., Addison-Wesley, 1995.

- [32] Brooks, R.A. A robust layered control system for a mobile robot. *IEEE Journal of Robotics and Automation*. 2(1), p. 14- 23, March, 1986.
- [33] Buschmann, F., Meunier, R., Rohnert, H., Sommerlad, P., and Stal, M. *Pattern-Oriented Software Architecture: A System of Patterns*. Wiley: Chichester, West Sussex, UK, 1996.
- [34] Bush, V. As we may think. *interactions*. 3(2), p. 35-46, 1996.
- [35] Carzaniga, A., Fuggetta, A., van der Hoek, A., Hall, R.S., Heimbigner, D.M., and Wolf, A.L. *A Characterization Framework for Software Deployment Technologies*. University of Colorado,Boulder, Report CU-CS-857-98, 1998, 1998.
- [36] Carzaniga, A., Rosenblum, D.S., and Wolf, A.L. Design and Evaluation of a Wide-Area Event Notification Service. *ACM Transactions on Computer Systems*. 9(3), p. 332-383, August, 2001.
- [37] Chapman, M.R.R. *In Search of Stupidity: Over 20 Years of High-Tech Marketing Disasters* 256 pgs., Apress, 2003.
- [38] Clements, P., Bachmann, F., Bass, L., Garlan, D., Ivers, J., Little, R., Nord, R., and Stafford, J. *Documenting Software Architectures: Views and Beyond*. Addison Wesley, 2002.
- [39] Clements, P., Kazman, R., and Klein, M. *Evaluating Software Architectures: Methods and Case Studies* 368 pgs., Addison-Wesley Professional, 2002.
- [40] Clements, P. and Northrop, L. *Software Product Lines: Practices and Patterns*. Addison-Wesley: New York, New York, 2002.
- [41] Clements, P.C. and Northrop, L.M. *Software Product Lines: Practices and Patterns*. The SEI Series in Software Engineering. Addison-Wesley Professional, 2001.
- [42] Coglianese, L., Smith, R., and Tracz, W. DSSA case study: navigation, guidance, and flight director design and development. In *Proceedings of the 1992 IEEE Symposium on Computer-Aided Control System Design*. p. 102-109, March, 1992.
- [43] Cohen, B. *Incentives Build Robustness in BitTorrent*. <<http://www.bittorrent.org/bittorrentecon.pdf>>, BitTorrent.org, 2003.
- [44] Collins-Sussman, B., Fitzpatrick, B.W., and Pilato, C.M. *Version Control with Subversion*. <<http://svnbook.red-bean.com/>>, HTML, 2004.
- [45] Colouriis, G., Dollimore, J., and Kindberg, T. *Distributed Systems: Concepts and Design*. 2nd. ed. Addison-Wesley, 1994.
- [46] Cook, J. and Orso, A. MonDe: Safe Updating through Monitored Deployment of New Component Versions. In *Proceedings of the 6th ESEC/FSE Workshop on Program Analysis for Software Tools and Engineering*. Lisbon, Portugal, September, 2005.
- [47] Coram, R. *Boyd: the Fighter Pilot Who Changed the Art of War*. Little, Brown, and Company, 2002.
- [48] Curtis, B., Krasner, H., and Iscoe, N. A Field Study of the Software Design Process for Large Systems. *Communications of the ACM*. 31(11), p. 1268-1287, November, 1988.
- [49] Damiani, E., di Vimercati, S.D.C., Paraboschi, S., Samarati, P., and Violante, F. A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer

- Networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*. Washington DC, November, 2002.
- [50] Dashofy, E. *xADL 2.0 Distilled: A Guide for Users of the xADL 2.0 Language*. <<http://www.isr.uci.edu/projects/xarchuci/guide.html>>, Webpage, 2003.
- [51] Dashofy, E., van der Hoek, A., and Taylor, R.N. A Comprehensive Approach for the Development of Modular Software Architecture Description Languages. *ACM Transactions on Software Engineering and Methodology (TOSEM)*. 14(2), p. 199-245, April, 2005.
- [52] Dashofy, E.M., Medvidovic, N., and Taylor, R.N. Using Off-the-Shelf Middleware to Implement Connectors in Distributed Software Architectures. In *Proceedings of the 21st International Conference on Software Engineering (ICSE'99)*. p. 3-12, Los Angeles, CA, May 16-22, 1999. <<http://portal.acm.org/citation.cfm?id=302407>>.
- [53] Dashofy, E.M. Issues in Generating Data Bindings for an XML Schema-Based Language. In *Proceedings of the Workshop on XML Technologies in Software Engineering (XSE 2001)*. Toronto, Canada, May 15, 2001.
- [54] Dashofy, E.M. and van der Hoek, A. Representing Product Family Architectures in an Extensible Architecture Description Language. In *Proceedings of the International Workshop on Product Family Engineering (PFE-4)*. p. 330-341, October, 2001.
- [55] Dashofy, E.M. *Supporting Stakeholder-Driven, Multi-View Software Architecture Modeling*. Thesis. Information and Computer Science, University of California, Irvine, p. 294, 2007.
- [56] Dean, J. and Ghernawat, S. MapReduce: Simplified Data Processing on Large Clusters In *Proceedings of the OSDI'04: Sixth Symposium on Operating System Design and Implementation*. San Francisco, CA, December, 2004, 2004.
- [57] DeLine, R. Avoiding packaging mismatch with flexible packaging. *IEEE Transactions on Software Engineering*. 27(2), p. 124-143, 2001.
- [58] DeRemer, F. and Kron, H.H. Programming-in-the-Large versus Programming-in-the-Small. *IEEE Transactions on Software Engineering*. 2(2), p. 80-86, June, 1976.
- [59] Deutsch, P. and Gosling, J. *The Eight Fallacies of Distributed Computing*. <<http://blogs.sun.com/jag/resource/Fallacies.html>>, 1994.
- [60] Devanbu, P.T. and Stubblebine, S. Software engineering for security: a roadmap. In *Proceedings of the Proceedings of the Conference on The Future of Software Engineering*. p. 227-239 ACM Press. Limerick, Ireland, 2000. <<http://doi.acm.org/10.1145/336512.336559>>.
- [61] Di Nitto, E. and Rosenblum, D.S. Exploiting ADLs to Specify Architectural Styles Induced by Middleware Infrastructures. In *Proceedings of the 21st International Conference on Software Engineering*. p. 13-22, IEEE Computer Society. Los Angeles, CA, May, 1999. <<http://portal.acm.org/citation.cfm?id=302406>>.
- [62] Dilley, J., Maggs, B., Parikh, J., Prokop, H., Sitaraman, R., and Weihl, B. Globally distributed content delivery. *IEEE Internet Computing*. 6(5), p. 50-58, September, 2002, 2002.

- [63] Dillinger, M., Madani, K., and Alonistioti, N. *Software Defined Radio: Architectures, Systems and Functions*. Wiley, 2003.
- [64] Dillon, L.A., Kutty, G., Melliar-Smith, P.M., Moser, L.E., and Ramakrishna, Y.S. Graphical Specifications for Concurrent Software Systems. In *Proceedings of the 14th International Conference on Software Engineering*. p. 214-224, Melbourne, Australia, May, 1992, 1992.
- [65] Dinda, P., Gross, T., Karrer, R., and Lowekamp, B. The Architecture of the Remos System. In *Proceedings of the IEEE International Symposium on High Performance Distributed Computing (HPDC 2001)*. San Francisco, CA, August, 2001.
- [66] Dobrica, L. and Niemela, E. A Survey on Software Architecture Analysis Methods. *IEEE Transactions on Software Engineering*. 28(7), p. 638-53, 2002.
- [67] DoD Architecture Framework Working Group. *DoD Architecture Framework, Version 1.0*. United States Department of Defense, Report, February 9, 2004. <[http://www.defenselink.mil/nii/doc/DoDAF\\_v1\\_Volume\\_1.pdf](http://www.defenselink.mil/nii/doc/DoDAF_v1_Volume_1.pdf)>.
- [68] Doherty, P., Haslum, P., Heintz, F., Merz, T., Nyblom, P., Persson, T., and Wingman, B. A Distributed Architecture for Autonomous Unmanned Aerial Vehicle Experimentation. In *Proceedings of the 7th International Symposium on Distributed Autonomous Systems*. 2004. <<http://www.ida.liu.se/~frehe/publications/dars2004.pdf>>.
- [69] Emmerich, W. *Engineering Distributed Objects*. 390 pgs., Wiley, 2000.
- [70] Eyles, D. Tales from the Lunar Module Guidance Computer. In *27th Annual Guidance and Control Conference of the American Astronautical Society (AAS)*. Breckenridge, Colorado, 2004. <[http://www.klabs.org/history/apollo\\_11\\_alarms/eyles\\_2004.htm](http://www.klabs.org/history/apollo_11_alarms/eyles_2004.htm)>.
- [71] Farrache, G. *bbFTP*. <<http://doc.in2p3.fr/bbftp>>, Website, 2005.
- [72] Feijis, L. and De Jong, R. 3D Visualization of Software Architectures. *Communications of the ACM*. 41(12), p. 73-78, December, 1998. <<http://portal.acm.org/citation.cfm?id=290151>>.
- [73] Feiler, P.H., Lewis, B., and Vestal, S. The SAE Avionics Architecture Description Language (AADL) Standard: A Basis for Model-Based Architecture-Driven Embedded Systems Engineering. In *Proceedings of the RTAS 2003 Workshop on Model-Driven Embedded Systems*. Washington, D.C., May, 2003.
- [74] Fielding, R., Gettys, J., Mogul, J.C., Frystyk, H., Masinter, L., Leach, P., and Berners-Lee, T. *Hypertext Transfer Protocol -- HTTP/1.1*. Internet Engineering Task Force, Request for Comments Report 2616, June, 1999.
- [75] Fielding, R.T. *Architectural Styles and the Design of Network-based Software Architectures*. Ph.D. Thesis. Information and Computer Science, University of California, Irvine, 2000. <<http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm>>.
- [76] Fielding, R.T. and Taylor, R.N. Principled Design of the Modern Web Architecture. *ACM Transactions on Internet Technology (TOIT)*. 2(2), p. 115-150, May, 2002.
- [77] Finkelstein, A. *The Future of Software Engineering 2000*. 381 pgs., ACM Press: New York, 2000.

- [78] Firby, R.J. *Adaptive execution in complex dynamic worlds*. Doctoral Thesis. Computer Science, Yale University, 1989.
- [79] Fogel, K. *Open Source Development with CVS*. Coriolis: Scottsdale, 1999.
- [80] Foote, B. and Yoder, J. Big Ball of Mud. In *Proceedings of the Fouth Conference on Patterns Languages of Programs (PLoP97/EuroPLoP97)*, p. 21 pages., Technical Report #WUCS-97-34, Department of Computer Science, Washington University. Monticello, Illinois, 1997. <<http://st-www.cs.uiuc.edu/users/hanmer/PLoP-97/Proceedings/foote.pdf>>.
- [81] Formal Systems (Europe) Ltd. *Failures-Divergence Refinement: FDR2 Users Manual*. 82 pgs., 2005.
- [82] Foster, I., Kesselman, C., and Tuecke, S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. *International Journal of High Performance Computing Applications*. 15(3), p. 200-222, 2001.
- [83] Fuggetta, A., Picco, G.P., and Vigna, G. Understanding Code Mobility. *IEEE Transactions on Software Engineering*. 24(5), p. 342-361, May, 1998.
- [84] Gambetta, D. *Trust*. Gambetta, D. ed. Blackwell: Oxford, 1990.
- [85] Gamma, E., Helm, R., Johnson, R., and Vlissides, J. *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley Professional Computing Series. Addison-Wesley Professional: Reading, MA, 1995.
- [86] Garlan, D., Allen, R., and Ockerbloom, J. Exploiting Style in Architectural Design Environments. In *Proceedings of the 2nd ACM SIGSOFT '94 Second Symposium on the Foundations of Software Engineering*. p. 175-188, ACM Press. New Orleans, LA, December 6-9, 1994.
- [87] Garlan, D., Allen, R., and Ockerbloom, J. Architectural Mismatch or Why It's Hard to Build Systems out of Existing Parts. In *Proceedings of the Seventeenth International Conference on Software Engineering (ICSE)*. p. 179-185, ACM. 1995.
- [88] Garlan, D., Allen, R., and Ockerbloom, J. Architectural Mismatch: Why Reuse Is So Hard. *IEEE Software*. 12(6), p. 17-26, November, 1995.
- [89] Garlan, D., Monroe, R.T., and Wile, D. ACME: An Architecture Description Interchange Language. In *Proceedings of the CASCON '97*. p. 169-183, IBM Center for Advanced Studies. Toronto, Ontario, Canada, November, 1997. <<http://www-2.cs.cmu.edu/afs/cs/project/able/ftp/acme-cascon97/acme-cascon97.pdf>>.
- [90] Garlan, D., Monroe, R.T., and Wile, D. ACME: Architectural Description of Component-Based Systems. In *Foundations of Component-Based Systems*. Leavens, G.T. and Sitaraman, M. eds. p. 47-68, Cambridge University Press, 2000.
- [91] Garlan, D., Cheng, S., and Schmerl, B. Increasing System Dependability through Architecture-based Self-repair. In *Architecting Dependable Systems* Lemos, R.d., Gacek, C., and Romanovsky, A. eds., 2003.
- [92] Gasser, M. *Building a secure computer system*. Van Nostrand Reinhold Co., 1988.
- [93] Georgas, J.C. and Taylor, R.N. Towards a Knowledge-based Approach to Architectural Adaptation Management. In *Proceedings of the 1st ACM SIGSOFT*

- Workshop on Self-managed Systems (WOSS '04).* p. 59-63, ACM Press. Newport Beach, CA, October, 2004.
- [94] Georgas, J.C., van der Hoek, A., and Taylor, R.N. Architectural Runtime Configuration Management in Support of Dependable Self-Adaptive Software. In *Proceedings of the Workshop on Architecting Dependable Systems (WADS '05), in conjunction with ICSE 2005.* p. 48-53, St. Louis, MO, 2005.
- [95] Ghemawat, S., Gobioff, H., and Leung, S.-T. The Google File System. In *Proceedings of the Proceedings of the 19th ACM Symposium on Operating Systems Principles.* ACM. Bolton Landing, New York, USA, 2003.
- [96] Ghezzi, C., Jazayeri, M., and Mandrioli, D. *Fundamentals of Software Engineering.* Second ed. 604 pgs., Prentice Hall Pearson Education, Inc.: Upper Saddle River, New Jersey, 2003.
- [97] Gokhale, S. Architecture-Based Software Reliability Analysis: Overview and Limitations. *IEEE Transactions on Dependable and Secure Computing.* 4(1), January-March 2007, 2007.
- [98] Goldman, N. and Balzer, R. The ISI Visual Design Editor Generator. In *Proceedings of the IEEE Symposium on Visual Languages.* p. 20-27, Tokyo, 1999.
- [99] Gomaa, H. *Designing Software Product Lines with UML: From Use Cases to Pattern-Based Software Architectures.* 736 pgs., Addison-Wesley Professional, 2004.
- [100] Gomaa, H. and Hussein, M. Software reconfiguration patterns for dynamic evolution of software architectures. In *Proceedings of the Proceedings of the Fourth Working IEEE/IFIP Conference on Software Architecture.* p. 79-88, 2004. <<http://ieeexplore.ieee.org/iel5/9167/29100/01310692.pdf?isnumber=29100>>[S TD&arnumber=1310692&arnumber=1310692&arSt=+79&ared=+88&arAuthor=Gomaa%2C+H,%3B+Hussein%2C+M].
- [101] Gorlick, M.M. and Razouk, R.R. Using Weaves for Software Construction and Analysis. In *Proceedings of the 13th International Conference on Software Engineering.* p. 23-34, May, 1991.
- [102] Gröne, B., Knöpfel, A., and Kugel, R. Architecture recovery of Apache 1.3 -- A case study. In *Proceedings of the 2002 International Conference on Software Engineering Research and Practice.* Las Vegas, 2002. <[http://f-m-c.org/publications/download/groene\\_et\\_al\\_2002-architecture\\_recovery\\_of\\_apache.pdf](http://f-m-c.org/publications/download/groene_et_al_2002-architecture_recovery_of_apache.pdf)>.
- [103] Gröne, B., Knöpfel, A., Kugel, R., and Schmidt, O. *The Apache Modeling Project.* Hasse Plattner Institute for Software Systems Engineering, Report, July 5, 2004. <[http://f-m-c.org/projects/apache/download/the\\_apache\\_modelling\\_project.pdf](http://f-m-c.org/projects/apache/download/the_apache_modelling_project.pdf)>.
- [104] Grosso, W. *Java RMI.* 1st ed. 572 pgs., O'Reilly Media, Inc., 2001.
- [105] Group, T.O. *Distributed Computing Environment Portal.* <<http://www.opengroup.org/dce/>>, 2005.
- [106] Guttag, J.V., Horning, J.J., and Wing, J.M. The Larch Family of Specification Languages. *IEEE Software.* 2(5), p. 24-36, September, 1985.

- [107] Guttman, B. and Roback, E. An Introduction to Computer Security: The NIST Handbook. Computer Systems Laboratory, N.I.O.S.A.T., Editor U.S. Government Printing Office, 1995.
- [108] Haas, R., Droz, P., and Stiller, B. Autonomic service deployment in networks. *IBM Systems Journal.* 42(1), p. 150-164, 2003.
- [109] Hall, R.S., Heimbigner, D., van der Hoek, A., and Wolf, A.L. An Architecture for Post-Development Configuration Management in a Wide-Area Network. In *Proceedings of the 1997 International Conference on Distributed Computing Systems.* p. 269-278, IEEE Computer Society. Baltimore, MD, May, 1997.
- [110] Hall, R.S., Heimbigner, D., and Wolf, A.L. A Cooperative Approach to Support Software Deployment Using the Software Dock. In *Proceedings of the 1999 International Conference on Software Engineering.* p. 174-183, ACM Press. Los Angeles, CA, May, 1999.
- [111] Harel, D. Statecharts: A Visual Formalism for Complex Systems. *Science of Computer Programming.* 8, p. 231-274, 1987.
- [112] Harold, E.R. *Java I/O.* 2nd ed. 726 pgs., O'Reilly Media, Inc., 2006.
- [113] Harrison, M.A., Ruzzo, W.L., and Ullman, J.D. Protection in operating systems. *Communications of the ACM.* 19(8), p. 461-471, 1976.
- [114] Hayes-Roth, B., Pfleger, K., Lalanda, P., Morigot, P., and Balabanovic, M. A Domain-Specific Software Architecture for Adaptive Intelligent Systems. *IEEE Transactions on Software Engineering.* 21(4), p. 288-301, April, 1995.
- [115] Heimdal, M.P.E. Safety and Software Intensive Systems: Challenges Old and New. In *Future of Software Engineering 2007* Briand, L. and Wolf, A. eds. p. 137-152, IEEE-CS Press, 2007.
- [116] Hendrickson, S.A., Dashofy, E.M., and Taylor, R.N. An Approach for Tracing and Understanding Asynchronous Architectures. Short paper. In *Proceedings of the 18th IEEE International Conference on Automated Software Engineering (ASE 2003).* p. 318-322, Montreal, Quebec, Canada, October 6-10, 2003.
- [117] Hendrickson, S.A., Dashofy, E.M., and Taylor, R.N. An Approach for Tracing and Understanding Asynchronous Architectures. In *Proceedings of the 18th IEEE International Conference on Automated Software Engineering (ASE 2003).* p. 318-322, Montreal, Quebec, Canada, October 6-10, 2003.
- [118] Hendrickson, S.A., Dashofy, E.M., and Taylor, R.N. An (Architecture-Centric) Approach for Tracing, Organizing, and Understanding Events in Event-Based Software Architectures. In *Proceedings of the 13th International Workshop on Program Comprehension, in conjunction with ICSE 2005.* p. 227-236, St. Louis, MO, May 15-16, 2005.
- [119] Hendrickson, S.A. and van der Hoek, A. Modeling Product Line Architectures through Change Sets and Relationships. In *Proceedings of the 29th International Conference on Software Engineering (ICSE 2007).* Minneapolis, MN, May 20-26, 2007.
- [120] Hirsch, D., Uchitel, S., and Yankelevich, D. Towards a Periodic Table of Connectors. In *Proceedings of the Simposio en Tecnología de Software.* Buenos Aires, Argentina, 1999.
- [121] Hitchens, R. *Java NIO.* 312 pgs., O'Reilly Media, Inc., 2002.

- [122] Hoare, C.A.R. Communicating Sequential Processes. *Communications of the ACM*. 21(8), p. 666-677, August, 1978.
- [123] Hofmeister, C., Nord, R.L., and Soni, D. *Applied Software Architecture*. 432 pgs., Addison Wesley Longman, 1999.
- [124] Honeywell, I. *MetaH Evaluation and Support Site*. <<http://www.hic.honeywell.com/metah/>>, 1998.
- [125] Houston, P. *Building Distributed Applications with Message Queuing Middleware*. Microsoft Corporation, White Paper Report, p. 14, 1998. <<http://www.microsoft.com/ntserver/techresources/appserv/MSMQ/msmqdistributed.asp>>.
- [126] Hunt, G.C. and Scott, M.L. The Coign Automatic Distributed Partitioning System. In *Proceedings of the Proceedings of the 3rd Symposium on Operating Systems Design and Implementation*. USENIX. New Orleans, Louisiana, February, 1999, 1999.
- [127] IBM. *Autonomic Computing Manifesto*. <[http://www.research.ibm.com/autonomic/manifesto/autonomic\\_computing.pdf](http://www.research.ibm.com/autonomic/manifesto/autonomic_computing.pdf)>, PDF document, 2001.
- [128] IBM. *Autonomic Computing Architecture: A Blueprint for Managing Complex Computing Environments*. Whitepaper Report, 2002. <<http://www-3.ibm.com/autonomic/pdfs/ACwhitepaper1022.pdf>>.
- [129] IBM. *WebSphere MQ - Product Overview*. <<http://www-3.ibm.com/software/ts/mqseries/messaging/>>, IBM, Website, 2003.
- [130] IEEE-SA Standards Board. *IEEE Recommended Practice for Architectural Description of Software-Intensive Systems*. 23 pgs., The Institute of Electrical and Electronics Engineers, Inc.: New York, NY, 2000.
- [131] IEEE. *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries* : 610. p. 217, Institute of Electrical and Electronics Engineers: New York, 1991.
- [132] IEEE. *IEEE Std 1003.1, 2004 Edition*. Report, 2004. <[http://www.unix.org/version3/ieee\\_std.html](http://www.unix.org/version3/ieee_std.html)>.
- [133] Immonen, A. and Niemelä, E. Survey of reliability and availability prediction methods from the viewpoint of software architecture. *Springer Journal of Software and System Modeling*. Published online, January 12, 2007, 2007.
- [134] InstallShield Corporation. *InstallShield*. <<http://www.installshield.com/>>, HTML, 2000.
- [135] ISO. Lotos, A Formal Description Technique Based on the Temporal Ordering of Observational Behavior. (ISO 8807), 1989.
- [136] ISO/IEC. *Information technology - Open Distributed Processing - Reference model*. ISO/IEC, Report 10746, December 15, 1998.
- [137] Jackson, D. Alloy: A Lightweight Object Modelling Notation. *ACM Transactions on Software Engineering and Methodology (TOSEM)*. 11(2), p. 256-290, April, 2002.
- [138] Jackson, M. *Software Requirements & Specifications: A Lexicon of Practice, Principles and Prejudices*. 228 pgs., ACM Press/Addison-Wesley, 1995.
- [139] Jackson, M. Problem Analysis and Structure. In *Proceedings of the Engineering Theories of Software Construction*. NATO Summer School. p. 3-20, IOS Press,

- Marktoberdorf, Germany, August, 2000, 2000. <<http://mcs.open.ac.uk/mj665/MarktCh3.pdf>>.
- [140] Jackson, M. *Problem Frames*. Addison-Wesley Professional: Reading, MA, 2001.
- [141] Jackson, M. *Michael Jackson -- Consultancy & Research in Software Development. Past Research Topics*. <<http://mcs.open.ac.uk/mj665/topics.html>>, Website, 2007.
- [142] Jacobson, I. *Object-Oriented Software Engineering: A Use Case Driven Approach*. 1st ed. 552 pgs., Addison-Wesley Professional, 1992.
- [143] JavaSoft. *JavaBeans 1.0 API Specification*. Sun Microsystems, Inc., Report version 1.00-A, December 4, 1996.
- [144] JavaSoft. *Java Message Service API*. Sun Microsystems, Inc., Report Version 1.0.2b, August 27, 2001. <<http://java.sun.com/products/jms/docs.html>>.
- [145] Jones, J.C. *Design Methods: Seeds of Human Futures*. John Wiley & Sons, Ltd.: New York, 1970.
- [146] Jones, J.C. *Design Methods*. 2nd ed. 472 pgs., John Wiley & Sons, Inc.: New York, NY, 1992.
- [147] Kan, G. *Gnutella*. In *Peer-to-Peer: Harnessing the Power of Disruptive Technologies* Oram, A. ed. p. 94-122, O'Reilly, 2001.
- [148] Kang, K.C., Cohen, S.G., Hess, J.A., Novak, W.E., and Peterson, A.S. *Feature-Oriented Domain Analysis (FODA) Feasibility Study*. Software Engineering Institute, Technical Report CMU/SEI-90-TR-21, November, 1990.
- [149] Kelley, T., Littman, J., and Peters, T. *The Art of Innovation: Lessons in Creativity from IDEO, America's Leading Design Firm*. Currency/Doubleday: New York, 2001.
- [150] Kephart, J.O. and Chess, D.M. The Vision of Autonomic Computing. *IEEE Computer*. 36(1), p. 41-50, January, 2003, 2003.
- [151] Kernighan, B.W. and Ritchie, D.M. *The C Programming Language*. 2nd ed. Prentice Hall, 1988.
- [152] Kichikaylo, T., Ivan, A., and Karamchetti, V. Constrained Component Deployment in Wide-Area Networks Using AI Planning Techniques. In *Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS'03)*. p. 10 pp., 2003.
- [153] Klusener, A.S., R, L., mmel, and Verhoef, C. *Architectural modifications to deployed software*. 54 \, 143-211 \ pgs., Elsevier North-Holland, Inc, 2005.
- [154] Kramer, J. and Magee, J. Change management of distributed systems. In *Proceedings of the Proceedings of the 3rd workshop on ACM SIGOPS European workshop: Autonomy or interdependence in distributed systems?* p. 1-4, ACM Press. Cambridge, United Kingdom, 1988. <<http://doi.acm.org/10.1145/504092.504113>>.
- [155] Kramer, J. and Magee, J. The Evolving Philosophers Problem: Dynamic Change Management. *IEEE Transactions on Software Engineering*. 16(11), p. 1293-1306, 1990. <<http://citeseer.nj.nec.com/rd/0%2C29040%2C1%2C0.25%2CDownload/http://citeseer.nj.nec.com/cache/papers/cs/4417/ftp:zSzzSzdsse.doc.ic.ac.ukzSzdsse-paperszSzconiczSzchange.pdf/kramer90evolving.pdf>>.

- [156] Kruchten, P. Mommy: Where Do Software Architectures Come From? In *Proceedings of the 1st International Workshop on Architectures for Software Systems*. Seattle, WA, April, 1995.
- [157] Kruchten, P. The Software Architect -- and the Software Architecture Team. In *Proceedings of the Software Architecture. Proceedings of TC2 First Working IFIP Conference on Software Architecture*. p. 565-583, Kluwer Academic Publishers. San Antonio, Texas, 1999.
- [158] Kruchten, P. *The Rational Unified Process: An Introduction*. Addison-Wesley Professional: Reading, MA, 2000.
- [159] Kruchten, P. *The Rational Unified Process: An Introduction*. 3rd ed. 320 pgs., 2003.
- [160] Lampson, B.W. Protection. *ACM SIGOPS Operating Systems Review*. 8(1), p. 18-24, 1974.
- [161] Larman, C. *Applying UML and Patterns. An Introduction to Object-Oriented Analysis and Design and the Unified Process*. 2nd ed. Prentice-Hall PTR, 2002.
- [162] Lazowska, E.D., Zahorjan, J., Graham, G.S., and Sevcik, K.C. *Quantitative system performance: computer system analysis using queueing network models*. Prentice-Hall, Inc.: Upper Saddle River, NJ, 1984.
- [163] Lee, S., Sherwood, R., and Bhattacharjee, B. Cooperative peer groups in NICE. In *Proceedings of the IEEE Infocom*. San Francisco, USA, April 1-3, 2003.
- [164] Leveson, N.G. *Safeware: System Safety and Computers*. 704 pgs., Addison-Wesley Professional, 1995.
- [165] Liang, S. *Java Native Interface: Programmer's Guide and Specification*. 1st ed. Prentice Hall PTR, 1999.
- [166] Littlewood, B. and Stringini, L. Software Reliability and Dependability: A Roadmap. In *Proceedings of the The Future of Software Engineering 2000*. p. 175-188, ACM Press. Limerick, Ireland, 2000.
- [167] Liu, C.L. and Layland, J.W. Scheduling Algorithms for Multiprogramming in a Hard-Real-Time Environment *Journal of the ACM (JACM)*. 20(1), p. 46-61, 1973.
- [168] Luckham, D. *The Power of Events: An Introduction to Complex Event Processing in Distributed Enterprise Systems*. 400 pgs., Addison-Wesley, 2002.
- [169] Luckham, D.C. and Henke, F.W.v. An Overview of Anna, a Specification Language for Ada. *IEEE Software*. 2(2), p. 9-23, March, 1985.
- [170] Luckham, D.C., Kenney, J.J., Augustin, L.M., Vera, J., Bryan, D., and Mann, W. Specification and Analysis of System Architecture Using Rapide. *IEEE Transactions on Software Engineering*. 21(4), p. 336-355, April, 1995. <<http://citeseer.nj.nec.com/luckham95specification.html>>.
- [171] Luckham, D.C. and Vera, J. An Event-Based Architecture Definition Language. *IEEE Transactions on Software Engineering*. 21(9), p. 717-734, September, 1995.
- [172] Lutz, R. Software Engineering for Safety: A Roadmap. In *Proceedings of the The Future of Software Engineering 2000*. p. 213-224, ACM Press. Limerick, Ireland, 2000.
- [173] Lyu, M. Software Reliability Engineering: A Roadmap. In *Future of Software Engineering 2007* Briand, L. and Wolf, A. eds. p. 153-170, IEEE-CS Press, 2007.

- [174] Magee, J., Dulay, N., and Kramer, J. Regis: A Constructive Development Environment for Distributed Programs. *IEE/IOP/BCS Distributed Systems Engineering*. 1(5), p. 304-312, September, 1994.
- [175] Magee, J., Dulay, N., Eisenbach, S., and Kramer, J. Specifying Distributed Software Architectures. In *Proceedings of the 5th European Software Engineering Conference (ESEC 95)*. 989, p. 137-153, Springer-Verlag, Berlin, 1995. <<http://portal.acm.org/citation.cfm?id=651497>>.
- [176] Magee, J. and Kramer, J. Dynamic Structure in Software Architectures. In *Proceedings of the 4th ACM SIGSOFT Symposium on Foundations of Software Engineering*. p. 3-14, ACM SIGSOFT. San Francisco, CA, October 16-18, 1996.
- [177] Magee, J. and Kramer, J. *Concurrency: State Models and Java Programs*. 2nd ed. 434 pgs., Wiley, 2006.
- [178] Maier, M. and Rechtin, E. *The Art of Systems Architecting*. 2nd ed. 344 pgs., CRC Press: Boca Raton, FL, 2000.
- [179] Malek, S., Beckman, N., Mikic-Rakic, M., and Medvidovic, N. A Framework for Ensuring and Improving Dependability in Highly Distributed Systems. In *Architecting Dependable Systems III* Lemos, R.d., Gacek, C., and Romanowski, A. eds. Springer Verlag, 2005.
- [180] Malek, S., Mikic-Rakic, M., and Medvidovic, N. A Style-Aware Architectural Middleware for Resource Constrained, Distributed Systems. *IEEE Transactions on Software Engineering*. 31(3), p. 256-272, March, 2005. <<http://www.scf.usc.edu/~malek/papers/TSE05.pdf>>.
- [181] Malek, S., Seo, C., Ravula, S., Petrus, B., and Medvidovic, N. Reconceptualizing a Family of Heterogeneous Embedded Systems via Explicit Architectural Support. In *Proceedings of the Proceedings of the 29th International Conference on Software Engineering*. p. 591-601, IEEE Computer Society. 2007.
- [182] Manolescu, I., Brambilla, M., Ceri, S., Comai, S., and Fraternali, P. Model-driven design and deployment of service-enabled web applications. *ACM Transactions on Internet Technology (TOIT)*. 5(3), August, 2005.
- [183] Marsh, S. *Formalising Trust as a Computational Concept*. Thesis. Department of Mathematics and Computer Science, University of Stirling, 1994.
- [184] Mattmann, C., Malek, S., Beckman, N., Mikic-Rakic, M., Medvidovic, N., and Crichton, D. GLIDE: A Grid-based, Lightweight, Infrastructure for Data-intensive Environments. In *Proceedings of the European Grid Conference (EGC2005)*. p. 68-77, Amsterdam, The Netherlands, February 14th-16th, 2005, 2005.
- [185] Mattmann, C.A., Medvidovic, N., Ramirez, P.M., and Jakobac, V. Unlocking the Grid. In *Proceedings of the Component-Based Software Engineering: 8th International Symposium, CBSE 2005*. 3489, Lecture Notes in Computer Science. St. Louis, MO, USA, May 14-15, 2005., 2005.
- [186] Mattmann, C.A., Crichton, D.J., Medvidovic, N., and Hughes, S. A software architecture-based framework for highly distributed and data intensive scientific applications In *Proceedings of the Proceeding of the 28th international conference on Software engineering*. p. 721-730, ACM Press. Shanghai, China, 2006. <<http://doi.acm.org/10.1145/1134285.1134400>>.
- [187] Maybee, M.J., Heimbigner, D.M., and Osterweil, L.J. Multilanguage Interoperability in Distributed Systems. In *Proceedings of the 18th International*

- Conference on Software Engineering.* p. 451-463, IEEE Computer Society. Berlin, Germany, March, 1996.
- [188] Medvidovic, N., Oreizy, P., and Taylor, R.N. Reuse of Off-the-Shelf Components in C2-Style Architectures. In *Proceedings of the 19th International Conference on Software Engineering.* p. 692-700, ACM Press. Boston, MA, May, 1997.
- [189] Medvidovic, N. and Taylor, R.N. A Classification and Comparison Framework for Software Architecture Description Languages. *IEEE Transactions on Software Engineering.* 26(1), p. 70-93, January, 2000. Reprinted in Rational Developer Network: Seminal Papers on Software Architecture. Rational Software Corporation, <<http://www.rational.net/>>, 2001.
- [190] Medvidovic, N., Dashofy, E., and Taylor, R.N. Moving Architectural Description from Under the Technology Lamppost. *Information and Software Technology.* 49(1), p. 12-31, January, 2007.
- [191] Mehta, N.R., Medvidovic, N., and Phadke, S. Towards a Taxonomy of Software Connectors. In *Proceedings of the 2000 International Conference on Software Engineering.* p. 178-187, ACM Press. Limerick, Ireland, 4-11 June, 2000. <[http://sunset.usc.edu/classes/cs599\\_2000/Conn-ICSE2000.pdf](http://sunset.usc.edu/classes/cs599_2000/Conn-ICSE2000.pdf)>.
- [192] Microsoft Corporation. *PowerPoint Home Page - Microsoft Office Online.* <<http://office.microsoft.com/powerpoint>>, 2007.
- [193] Microsoft Corporation. *Visio Home Page - Microsoft Office Online.* <<http://office.microsoft.com/visio>>, 2007.
- [194] Mitra, N. *Simple Object Access Protocol (SOAP) 1.2: Primer.* <<http://www.w3.org/TR/soap12-part0/>>, W3C, HTML, 2003.
- [195] Modular Software-programmable Radio Consortium. *Software Communications Architecture Specification v2.2.* Specification Report MSRC-5000SCA, p. 165, November 17, 2001.
- [196] Monroe, R.T. *Capturing Software Architecture Design Expertise With Armani.* School of Computer Science, Carnegie Mellon University, Technical Report Report CMU-CS-98-163, October, 1998. <[http://www-2.cs.cmu.edu/~able/paper\\_abstracts/armani-lrm.html](http://www-2.cs.cmu.edu/~able/paper_abstracts/armani-lrm.html)>.
- [197] Moriconi, M., Qian, X., and Riemenschneider, R.A. Correct Architecture Refinement. *IEEE Transactions on Software Engineering.* 21(4), p. 356-372, 1995. <<http://www.computer.org/tse/ts1995/e0356abs.htm>>.
- [198] Mos, A. and Murphy, J. COMPAS: Adaptive Performance Monitoring of Component-Based Systems. In *Proceedings of the Workshop on Remote Analysis and Measurement of Software Systems (RAMSS).* Edinburgh, Scotland, UK, May, 2004.
- [199] Mukerji, J. and Miller, J. eds. *MDA Guide Version 1.0.1.* Object Management Group, 2003.
- [200] Nelson, H.G. and Stolterman, E. *The Design Way: Intentional Change in an Unpredictable World - Foundations and Fundamentals of Design Competence.* Educational Technology Publications, Inc., 2003.
- [201] Nemhauser, G.L. and Wolsey, L.A. *Integer and combinatorial optimization.* Wiley-Interscience: New York, NY, 1988.
- [202] Nesnas, I.A.D., Simmons, R., Gaines, D., Kunz, C., Diaz-Calderon, A., Estlin, T., Madison, R., Guineau, J., McHenry, M., Shu, I.-H., and Apfelbaum, D.

- CLARAty: Challenges and Steps Toward Reusable Robotic Software. *International Journal of Advanced Robotic Systems.* 3(1), p. 23-30, 2006.
- [203] Ng, K., Kramer, J., and Magee, J. A CASE Tool for Software Architecture Design. *Journal of Automated Software Engineering.* 3, p. 261-284, August, 1996.
- [204] Nilsson, N.J. *Principles of Artificial Intelligence.* Tioga Publishing Company, 1980.
- [205] Norman, D.A. *The Design of Everyday Things.* 1st Basic paperback ed. 272 pgs., Basic Books: New York, 2002.
- [206] Nuseibeh, B. and Easterbrook, S. Requirements engineering: a roadmap. In *Proceedings of the Conference on The Future of Software Engineering* p. 35-46, ACM Press. Limerick, Ireland 2000.
- [207] Nuseibeh, B. Weaving Together Requirements and Architectures. *IEEE Computer.* 34(2), p. 115-117, March, 2001, 2001.
- [208] OASIS. *eXtensible Access Control Markup Language (XACML).* <[http://docs.oasis-open.org/xacml/2.0/access\\_control-xacml-2.0-core-spec-os.pdf](http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf)>, OASIS, 2005.
- [209] Object Management Group. ed. *The Common Object Request Broker: Architecture and Specification.* 946 pgs., Object Management Group, 2001.
- [210] Object Management Group. *OMG XML Metadata Interchange (XMI) Specification.* <<http://www.omg.org/cgi-bin/doc?formal/02-01-01.pdf>>, PDF, 2002.
- [211] Object Management Group. *Meta Object Facility (MOF) Specification.* <<http://www.omg.org/cgi-bin/doc?formal/02-04-03.pdf>>, PDF, 2002.
- [212] Object Management Group. *UML Profile for DODAF/MODAF (UPDM) Request for Proposal.* OMG, RFP Report syseng/05-08-01, August 22, 2005.
- [213] Ommering, R.v., Linden, F.v.d., Kramer, J., and Magee, J. The Koala Component Model for Consumer Electronics Software. *IEEE Computer.* 33(3), p. 78-85, March, 2000.
- [214] Oreizy, P. Issues in Modeling and Analyzing Dynamic Software Architectures. In *Proceedings of the International Workshop on the Role of Software Architecture in Testing and Analysis.* Marsala, Sicily, Italy, June 30-July 3, 1998.
- [215] Oreizy, P., Medvidovic, N., and Taylor, R.N. Architecture-Based Runtime Software Evolution. In *Proceedings of the 20th International Conference on Software Engineering (ICSE '98).* p. 177-186, IEEE Computer Society. Kyoto, Japan, April, 1998. <<http://www.ics.uci.edu/~peymano/papers/ICSE98.pdf>>.
- [216] Oreizy, P., Gorlick, M.M., Taylor, R.N., Heimbigner, D., Johnson, G., Medvidovic, N., Quilici, A., Rosenblum, D.S., and Wolf, A.L. An Architecture-based Approach to Self-Adaptive Software. *IEEE Intelligent Systems.* 14(3), p. 54-62, May-June, 1999.
- [217] Orfali, R., Harkey, D., and Edwards, J. *The Essential Distributed Objects Survival Guide.* Wiley: New York, NY, 1996.
- [218] Orso, A., Liang, D., Harrold, M.J., and Lipton, R. Gamma System: Continuous Evolution of Software after Deployment. In *Proceedings of the International Symposium on Software Testing and Analysis (ISSTA 2002).* Rome, Italy, July, 2002.

- [219] Parnas, D.L. On the Criteria to be Used in Decomposing Systems into Modules. *Communications of the ACM*. 15(12), p. 1053-1058, 1972.
- [220] Perry, D.E. Software Interconnection Models. In *Proceedings of the 9th International Conference on Software Engineering (ICSE)*. p. 61-69, IEEE Computer Society. March, 1987.
- [221] Perry, D.E. and Wolf, A.L. Foundations for the Study of Software Architecture. *ACM SIGSOFT Software Engineering Notes*. 17(4), p. 40-52, October, 1992.
- [222] Peter, L.J. and Hull, R. *The Peter Principle: why things always go wrong*. 179 pgs., William Morrow & Company, Inc.: New York, 1969.
- [223] Petroski, H. *To Engineer is Human*. St. Martin's Press 1985.
- [224] Petroski, H. *The Evolution of Useful Things*. Alfred A. Knopf, Inc., 1992.
- [225] Petroski, H. *Design Paradigms: Case histories of error and judgement in engineering*. Cambridge University Press 1994.
- [226] Petroski, H. *Invention by Design: How engineers get from thought to thing*. Harvard University Press, 1996.
- [227] Pezze, M. and Young, M. *Software Testing and Analysis: Process, Principles, and Techniques*. 488 pgs., Wiley, 2007.
- [228] Pfleeger, C.P. and Pfleeger, S.L. *Security in Computing*. Third ed. 976 pgs., Prentice Hall PTR, 2003.
- [229] Pohl, K., Böckle, G., and van der Linden, F.J. *Software Product Line Engineering: Foundations, Principles and Techniques*. 1 ed. 468 pgs., Springer: New York, New York, 2005.
- [230] Pollio, M.V. *On Architecture*. <http://penelope.uchicago.edu/Thayer/E/Roman/Texts/Vitruvius/home.html>, Website.
- [231] Polya, G. *How to Solve It: A New Aspect of Mathematical Method*. Second ed. 253 pgs., Princeton University Press, 1957.
- [232] Pooley, R. Software Engineering and Performance: A Roadmap. In *Proceedings of the The Future of Software Engineering 2000*. p. 189-200, ACM Press. Limerick, Ireland, 2000.
- [233] Rabiner, L.R. A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition. *Proceedings of the IEEE*. 77(2), p. 257-286, February 1989, 1989.
- [234] Raggett, D., Le Hors, A., and Jacobs, I. *HTML 4.01 Specification*. W3C, Report, December 24, 1999. <<http://www.w3.org/TR/html401/>>.
- [235] Rapanotti, L., Hall, J., Jackson, M., and Nuseibeh, B. Architecture Driven Problem Decomposition. In *Proceedings of the 12th IEEE International Requirements Engineering Conference (RE'04)*. p. 80-89, IEEE. Kyoto, Japan, September, 2004, 2004.
- [236] Rational Software Corporation. *Model-Driven Development with UML: Rational Rose*. <[http://www.rational.com/media/products/rose/D185H\\_Rose.pdf](http://www.rational.com/media/products/rose/D185H_Rose.pdf)>, PDF, 2002.
- [237] Rational Software Corporation. *Rational Rose: Using Rose*. IBM Corporation, Report 800-024462-000, p. 258, 2003. <[ftp://ftp.software.ibm.com/software/rational/docs/v2003/win\\_solutions/rational\\_rose/rose\\_user.pdf](ftp://ftp.software.ibm.com/software/rational/docs/v2003/win_solutions/rational_rose/rose_user.pdf)>.

- [238] Reenskaug, T. *Thing-Model-View-Editor - an example from a planning system*. Xerox PARC (Technical Note), Technical note Report, May, 1979. <<http://heim.ifi.uio.no/~trygver/themes/mvc-background/index.html>>.
- [239] Reenskaug, T. The Model-View-Controller (MVC): Its Past and Present. In *Proceedings of the Java and Object-Oriented Software Engineering (JAOO)*. Aarhus, Denmark, 22-25 September, 2003. <[http://heim.ifi.uio.no/~trygver/2003/javazone-jaoo/MVC\\_pattern.pdf](http://heim.ifi.uio.no/~trygver/2003/javazone-jaoo/MVC_pattern.pdf)>.
- [240] Reiss, S.P. Connecting Tools Using Message Passing in the Field Environment. *IEEE Software*. 7(4), p. 57-66, July, 1990.
- [241] Ren, J. and Taylor, R.N. Visualizing Software Architecture with Off-The-Shelf Components. In *Proceedings of the Fifteenth International Conference on Software Engineering and Knowledge Engineering (SEKE 2003)*. p. 132-141, San Francisco, CA, July 1-3, 2003.
- [242] Ren, J., Taylor, R., Dourish, P., and Redmiles, D. Towards An Architectural Treatment of Software Security: A Connector-Centric Approach. In *Proceedings of the Workshop on Software Engineering for Secure Systems (SESS 05), in conjunction with ICSE 2005*. St. Louis, MO, May, 2005.
- [243] Ren, J. and Taylor, R.N. A Secure Software Architecture Description Language. In *Proceedings of the Workshop on Software Security Assurance Tools, Techniques, and Metrics, Co-located with the 20th IEEE/ACM International Conference on Automated Software Engineering (ASE 2005)*. Long Beach, CA, 2005.
- [244] Robbins, J., Medvidovic, N., Redmiles, D., and Rosenblum, D. Integrating Architecture Description Languages with a Standard Design Method. In *Proceedings of the 20th International Conference on Software Engineering (ICSE)*. p. 209-218, ACM Press. Kyoto, Japan, April, 1998. <<http://www.isr.uci.edu/architecture/papers/TR-ICS-UCI-97-35.pdf>>.
- [245] Rosenthal, R., van der Hoek, A., Mikic-Rakic, M., and Medvidovic, N. Mae - A System Model and Environment for Managing Architectural Evolution. *ACM Transactions on Software Engineering and Methodology (TOSEM)*. 13(2), p. 240-276, April, 2004.
- [246] Rozanski, N. and Woods, E. *Software Systems Architecture: Working With Stakeholders Using Viewpoints and Perspectives* 576 pgs., Addison-Wesley Professional, 2005.
- [247] Rumbaugh, J., Blaha, M., Lorenzen, W., Eddy, F., and Premerlani, W. *Object-Oriented Modeling and Design*. 1st ed. Prentice Hall, 1990.
- [248] Sabbagh, K. *Skyscraper*. 388 pgs., Viking, 1989.
- [249] Saltzer, J.H. and Schroeder, M.D. The protection of information in computer systems. *Proceedings of the IEEE*. 63(9), p. 1278-308, 1975. <file:/l:/security/Classic/protection\_of\_info.pdf>.
- [250] Schach, S.R. *Object-Oriented & Classical Software Engineering*. Seventh ed. 618 pgs., McGraw Hill Higher Education, 2007.
- [251] Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Second ed. John Wiley & Sons, 1995.
- [252] Schneier, B. *Secrets and Lies: Digital Security in a Networked World*. 432 pgs., John Wiley & Sons, Inc., 2000.

- [253] Schön, D. *The Reflective Practitioner: How Professionals Think in Action.* 374 pgs., Basic Books, Inc. Publishers: New York, 1983.
- [254] Seo, C., Malek, S., and Medvidovic, N. An Energy Consumption Framework for Distributed Java-Based Systems. In *Proceedings of the Proceedings of the 22nd IEEE/ACM International Conference on Automated Software Engineering (ASE)*. Atlanta, Georgia, November, 2007, 2007.
- [255] Sessions, R. *COM and DCOM: Microsoft's Vision for Distributed Objects*. John Wiley & Sons Inc.: New York, New York, 1997.
- [256] Shaw, M. Procedure Calls Are the Assembly Language of Software Interconnection: Connectors Deserve First-Class Status. In *Studies of Software Design, Proceedings of a1993 Workshop* Lamb, D.A. ed. 1078, p. 17-32, Lecture Notes in Computer Science, Springer-Verlag, 1994.
- [257] Shaw, M., DeLine, R., Klein, D.V., Ross, T.L., Young, D.M., and Zelesnik, G. Abstractions for Software Architecture and Tools to Support Them. *IEEE Transactions on Software Engineering*. 21(4), p. 314-335, April, 1995. <<http://ieeexplore-beta.ieee.org/iel1/32/8744/00385970.pdf>>.
- [258] Shaw, M., DeLine, R., and Zelesnik, G. Abstractions and implementations for architectural connections. In *Proceedings of the Third International Conference on Configurable Distributed Systems*. p. 2-10, Annapolis, MD, USA, May, 1996.
- [259] Shaw, M. and Garlan, D. *Software Architecture: Perspectives on an Emerging Discipline*. 242 pgs., Prentice Hall, 1996.
- [260] Smolander, K. What is included in software architecture? A case study in three software organizations. In *Proceedings of the Ninth Annual IEEE International Conference and Workshop on the Engineering of Computer-Based Systems*. p. 131-138, 2002.
- [261] Smolander, K. and Päivärinta, T. Describing and Communicating Software Architecture in Practice: Observations on Stakeholders and Rationale. In *Proceedings of the Fourteenth International Conference on Advanced Information Systems Engineering (CAiSE'02)*. p. 117-133, Springer Berlin. Toronto, Ontario, Canada May 27-31, 2002, 2002.
- [262] Spencer, J. *Architecture Description Markup Language (ADML): Creating an Open Market for IT Architecture Tools*. The Open Group, White Paper Report, September 26, 2000. <<http://www.opengroup.org/tech/architecture/adml/background.htm>>.
- [263] Spitznagel, B. and Garlan, D. A compositional formalization of connector wrappers. In *Proceedings of the 25th International Conference on Software Engineering*. p. 374-384, 2003. <<file:///security/Other/01201216.pdf>>.
- [264] Spivey, J.M. *Understanding Z*. Cambridge University Press, 1988.
- [265] Stewart, W.J. *Introduction to Numerical Solution of Markov Chains*. Princeton University Press, 1994.
- [266] Suryanarayana, G., Erenkrantz, J.R., and Taylor, R.N. An Architectural Approach for Decentralized Trust Management. *IEEE Internet Computing*. 9(6), p. 16-23, November/December, 2005. <<http://doi.ieeecomputersociety.org/10.1109/MIC.2005.119>>.

- [267] Suryanarayana, G., Diallo, M.H., Erenkrantz, J.R., and Taylor, R.N. Architecting Trust-enabled Peer-to-Peer File-sharing Applications. *ACM Crossroads, issue on Software Engineering*. 12(4), p. 11-19, Summer, 2006.
- [268] Suryanarayana, G., Diallo, M.H., Erenkrantz, J.R., and Taylor, R.N. Architectural Support for Trust Models in Decentralized Applications. In *Proceedings of the 28th International Conference on Software Engineering*. p. 52-61, ACM Press. Shanghai, China, May, 2006. <<http://doi.acm.org/10.1145/1144359.1144364>>.
- [269] SysML Partners. *Systems Modeling Language (SysML) Specification version 0.9*. Report, p. 270, January 10, 2005. <<http://www.sysml.org/artifacts/spec/SysML-v0.9-PDF-050110R1.pdf>>.
- [270] SysML.org. *SysML Partners*. <<http://www.sysml.org/partners.htm>>, Webpage, 2007.
- [271] Szyperski, C. *Component Software: Beyond Object-Oriented Programming*. ACM Press: New York, 1997.
- [272] Szyperski, C. *Component Software - Beyond Object-Oriented Programming*. 2nd ed. Addison-Wesley, 2002.
- [273] Tanenbaum, A.S. and van Steen, M. *Distributed Systems: Principles and Paradigms*. 803 pgs., Prentice-Hall: Upper Saddle River, New Jersey, 2002.
- [274] Taylor, R., Tracz, W., and Coglianese, L. Software Development Using Domain-Specific Software Architectures. *Software Engineering Notes*. 20(5), December, 1995.
- [275] Taylor, R.N., Medvidovic, N., Anderson, K.M., E. James Whitehead, J., Robbins, J.E., Nies, K.A., Oreizy, P., and Dubrow, D.L. A Component- and Message-Based Architectural Style for GUI Software. *IEEE Transactions on Software Engineering*. 22(6), p. 390-406, June, 1996.
- [276] Taylor, R.N., Medvidovic, N., Anderson, K.M., Whitehead, E.J., Jr., Robbins, J.E., Nies, K.A., Oreizy, P., and Dubrow, D.L. A component- and message-based architectural style for GUI software. *IEEE Transactions on Software Engineering*. 22(6), p. 390-406, 1996.
- [277] Taylor, R.N. and van der Hoek, A. Software Design and Architecture The once and future focus of software engineering In *Future of Software Engineering (FOSE '07)* Wolf, A. and Briand, L. eds. p. 226-243, IEEE Computer Society, 2007. <<http://doi.ieeecomputersociety.org/10.1109/FOSE.2007.21>>.
- [278] Telecommunication Standardization Sector of ITU. *Specification and Description Language (SDL)*. Report ITU Standard Z.100, 2002. <<http://www.itu.int/ITU-T/studygroups/com17/languages/Z100.pdf>>.
- [279] Telelogic AB. *Telelogic System Architect for Creating Enterprise Architectures*. <<http://www.telelogic.com/popkin/>>, Website, 2007.
- [280] The Globus Alliance. *The Globus Alliance*. <<http://www.globus.org/>>, Website.
- [281] The Omni Group. *The Omni Group - Applications - OmniGraffle*. <<http://www.omnigroup.com/applications/omnigraffle/>>, 2007.
- [282] The Open Group. *TOGAF (The Open Group Architecture Framework) Version 8.1 "Enterprise Edition"*. The Open Group, Report, p. 349, December 19, 2003. <<http://www.opengroup.org/architecture/togaf8-doc/arch/>>.

