Trentino

SCA Runtime for Embedded Systems



Created by

Emeric Kwemou

|  |  |
| --- | --- |
| We acknowledge that this document uses material from the arc 42 architecture  template, <http://www.arc42.de>. Created by Dr. Peter Hruschka & Dr. Gernot Starke. |  |

**Revision History**

| **Version** | **Date** | **Reviser** | **Description** |
| --- | --- | --- | --- |
| 0.2 | 01.09.2012 |  |  |
| 0.7 | 12.06.2013 |  |  |
|  |  |  |  |

**Related documents**

|  |  |
| --- | --- |
| **Document** | **Description** |
| SCA | Service Component Architecture  Assembly Model Specification Version  1.1 |
| SCA CPP | Service Component Architecture Client and Implementation Model for C++ Specification Version 1.1 |

**Table of Contents**

1. Introduction and Goals 5

1.1 Business context 5

1.2 Requirements Overview 7

1.3 Quality Goals 8

1.4 Stakeholders 9

2. Architecture Constraints 9

2.1 Technical Constraints 9

2.2 Organizational Constraints 10

2.3 Conventions 11

3. System Scope and Context 11

3.1 Business Context 11

3.2 Technical Context 11

3.3 External Interfaces 11

4. Solution Strategy 14

5. Building Block View 14

5.1 Level 1 14

5.2 Level 2 15

5.3 Level 3 16

6. Runtime View 16

6.1 Runtime Scenario 1 16

6.2 Runtime Scenario 2 16

6.3 ... 16

6.4 Runtime Scenario n 16

7. Deployment View 16

7.1 Infrastructure Level 1 16

7.2 Infrastructure Level 2 17

8. Concepts 17

8.1 Domain Models 17

8.2 Recurring or Generic Structures and Patterns 17

8.3 Persistency 17

8.4 User Interface 17

8.5 Ergonomics 18

8.6 Flow of Control 18

8.7 Transaction Procession 18

8.8 Session Handling 18

8.9 Security 18

8.10 Safety 18

8.11 Communications and Integration 18

8.12 Distribution 18

8.13 Plausibility and Validity Checks 18

8.14 Exception/Error Handling 18

8.15 System Management and Administration 18

8.16 Logging, Tracing 18

8.17 Business Rules 18

8.18 Configurability 19

8.19 Parallelization and Threading 19

8.20 Internationalization 19

8.21 Migration 19

8.22 Testability 19

8.23 Scaling, Clustering 19

8.24 High Availability 19

8.25 Code Generation 19

8.26 Build-Management 19

9. Design Decisions 19

9.1 <Decision Topic 1> 19

9.2 <Decision Topic 2> 20

9.3 <Decision Topic 3> 20

... 20

10. Quality Scenarios 20

10.1 Quality Tree 20

10.2 Evaluation Scenarios 20

11. Technical Risks 20

12. Glossary 20

Remark: The Microsoft-Word™ variant of this template contains hidden remarks and suggestions. You can toggle display of this text by the appropriate Word-command.

# Introduction and Goals

## Business context

Picture 1: From business constraints to architectural constraints

Nowadays embedded systems development is facing rising complexity of the business domain. While the systems are becoming more and more complex, they have to fulfill time to market deadline and have to be as cheap as possible. In addition, systems often have to be easily embeddable in heterogeneous environment. Finally product development should quickly react to market changes or be as variable as possible to address different market segments. Those business constraints naturally have impact on architectures of the developed system. The use of SOA concepts and principles has helped to solve issues for the Enterprise resource platform level. We believe that SOA concepts principles can be used to solve the same issues we are facing in the embedded domain. Trentino is a platform that help the software architect fulfill those business requirements by:

1. Simplifying application management.
   1. Deploy, start stop or upgrade
   2. Enable creation of private clouds
2. Enabling optimal systems integration
   1. Vertical and horizontal
   2. Also integration in an Environment with SIL2/3 certified subsystems
3. Enabling high reusability of system components
4. Enabling product flexibility in that sense that many variations of the same product should be easily created
5. Focusing on resource and time constrained embedded systems controllers or field devices
   1. Running 24/7 days
   2. With high volume of data exchanged
   3. Local or distributed on many nodes
   4. predictable response time of components

Trentino is a lightweight and modular SOA runtime that is specifically designed for the peculiarities of the embedded domain. It is based on the open standard [Service Component Architecture (SCA)](http://www.oasis-opencsa.org/ci/c) and enables support for a variety of industrial protocols.

Trentino delivers a Tool and a Runtime to build, deploy and host applications compliant with the SCA specification.

Picture 2: target domain

Applications are typically controllers as part of a Distributed Control System or a SCADA. Applications can also be complex Sensors for Industry or Building Automation.

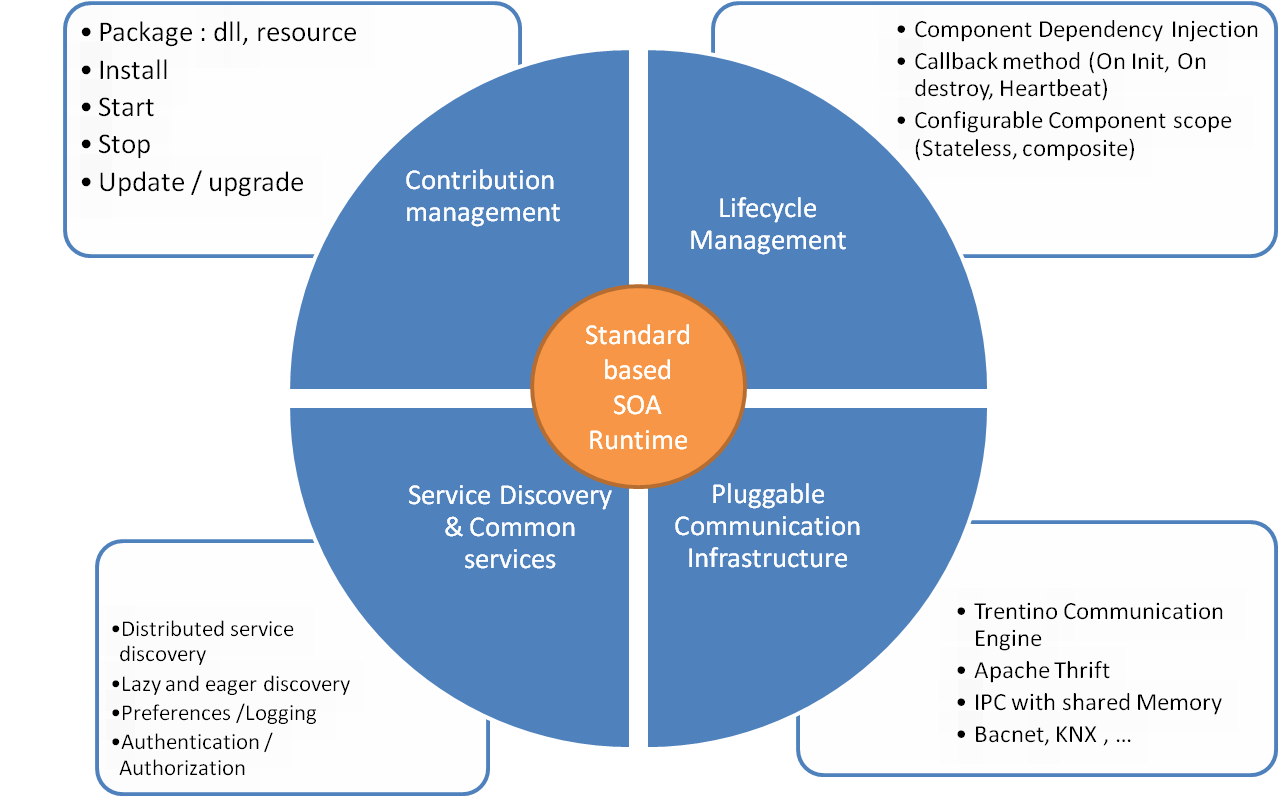
Picture 3: Applications make use of an OS

The introduction to the architecture documentation should list the driving forces that software architects must consider in their decisions.

This includes on the one hand the fulfillment of functional requirements of the stakeholders, on the other hand the fulfillment of or compliance with required constraints, always in consideration of the architecture goals.

## Requirements Overview

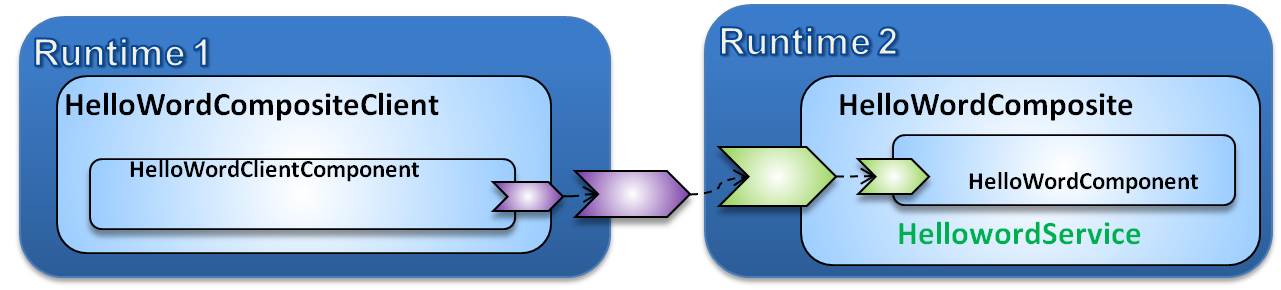
### Functional requirements



Picture 4: Trentino functions

1. Standard based SOA Runtime, implement SCA specification. Trentino aims to be fully compliant with SCA specification. Deviation from the specs might occur based on non functional requirements from the embedded domain.
2. Component Lifecycle management:
   1. Dependencies to a component can be automatically injected by the runtime
   2. Lifecycle callback methods can be defined and called by the runtime
   3. Scope of the component is configurable and managed by the runtime as defined by the SCA specification
3. Pluggable communication Infrastructure
   1. The runtime should enable plug in of new communication frameworks and protocols. A default communication framework is provided. An API for integrating new communication framework is also provided.
4. Service Discovery and Common services
   1. Platform should enable discovery of services distributed over different runtime nodes or provided by services not hosted on a Trentino runtime
   2. Common reusable services should be provided to speed up application development. Example services are :
      1. Data storage service
      2. Logging Service
      3. Authentication and authorization Services
5. Contribution management: Trentino should provide functions to manage applications, this includes starting, stopping and upgrading contributions

### Example



Picture 5: Assembly diagram of Helloworld

A SCA application called Helloword is developed in C++. It has a server and a client parts.

1. The server implements the HelloorldService in a HelloworldComponent that is part of the HelloworldComposite. The Client is also a component that implements no services but uses or calls the HelloworldService. Both client and server are part of the same application that is distributed over two separate Trentino runtimes and communicate using tcp/ip.
2. After client and server development, the system is described and configured used SCA service component description language.
3. Then Trentino tool is used to validate the application and generated extra artifacts used to manage the application.
4. Runtime 1 and 2 are started using the Trentino console
5. Then the application with all generated artifacts is deployed to both Trentino runtimes.

Short description of the functional requirements.

Digest (or abstract) of the requirements documents.

Reference to complete requirements documents (incl. version identification and location).

Contents

A compact summary of the functional environment of the system. Answers the following questions (at least approximately):

1. What happens in the system’s environment?
2. Why should the system exist? Why is the system valuable or important? Which problems does the system solve?

Motivation

From the point of view of the end users a system is created or modified to improve execution of a business activity.

This essential architecture driver must not be neglected even though the quality of an architecture is mostly judged by its level of fulfillment of non-functional requirements.

Form

Short textual description, probably in tabular use-case format.

The business context should in any case refer to the corresponding requirements documents.

Examples

Short descriptions of the most important:

1. business processes
2. functional requirements
3. non-functional requirements and other constraints (the most important ones must be covered as architecture goals or are listed in the “Constraints” section), and/or
4. quantity structures
5. background information

Here you can reuse parts of the requirements documents – but keep these excerpts short and balance readability against avoidance of redundancy.

## Quality Goals

The main objective of Trentino is to provide a component model for developing embedded systems. The main quality goals of Trentino platforms are mostly derived from the quality goals of applications hosted on Trentino.

Trentino defines a plugging mechanism used to integrate communication frameworks and protocols into Trentino. The quality goals of those pluggin are defined in the respective architecture documents.

Those goals are:

1. Availability: Application runs 24/7 days and no downtime is tolerated. Platform should simplify implementation of redundancy strategies to increase availability
2. Performance:
   1. Each application defines its own performance goals and chooses communication frameworks that match the required goals.
3. Determinism: For local communication between components, Trentino must guarantee that the time between a call on a proxy and its concrete execution on the target object is less than 100 micro second in 90% of the calls, for a set of environments to be defined before testing. This value is lower than the one requested by some known Trentino users.
4. Usability: Trentino is a framework to boost application development.
   1. It should be possible for end user to compile and deploy and application into a runtime in 5 minutes.
   2. It should be possible to create artifacts to writes tests for SCA components

Contents

The top three (max five) goals for the architecture and/or constraints whose fulfillment is of highest importance to the major stakeholders.

Goals that define the architecture’s quality could be:

1. availability
2. modifiability
3. performance
4. security
5. testability
6. usability

Motivation

If you as an architect do not know how the quality of your work can be judged …

Form

Simple tabular representation, ordered by priorities

Background Information

NEVER start developing an architecture if these goals have not been put into writing and have not been signed by the major stakeholders.

|  |
| --- |
| We have endured projects lacking defined quality goals much too often. We do not like to suffer, therefore we are by now highly convinced that the few hours spent on collecting quality goals are well invested.  PH & GS. |

Sources

The DIN/ISO 92000 Standard contains an extensive set of possible quality goals.

Or use chapters 10 – 17 of the VOLERE template as a starting point (www.volere.co.uk).  
PH

## Stakeholders

|  |  |
| --- | --- |
| OASIS | Define SCA API |
| Siemens AG and Sectors | Define requirements specific to Siemens products |
| Trentino community | Test and use Trentino, contribute with requirements |

Contents

A list of the most important persons or organizations that are affected by can contribute to the architecture.

Motivation

If you do not know the persons participating in or concerned with the project you may get nasty surprises later in the development process. Should your project manager maintain this list, make sure that all the people influencing the architecture are part of it.

Form

Simple table with role names, person names, their knowledge as pertaining to architecture, their availability, etc.

# Architecture Constraints

The most important constraint of the Trentino Platform is that it is hosted on a resource constrained environment, where some external parts have real time constraints or SIL compliance constraints. Trentino itself have SIL 0 constraints. So the constraints in summary are:

1. Application hosted on the platform should be able to communicate with external Processes or applications that are SIL 2 compliants, Trentino should not prevent those external application from being SIL 2 or tree compliant. The correct communiocation mechanism with those applications should be choosed
2. Application hosted on Trentino might have Soft real time requirements; Trentino should therefore enable determinist time behavior of the applications hosted on it.
3. The platform without hosted application should not consume more that 500 KB of the hosting device.
4. It should be possible the debug hosted applications as simple as without hosting it on the platform

Contents

Any requirement that constrains software architects in their freedom of design decisions or the development process.

Motivation

Architects should know exactly where they are free in their design decisions and where they must adhere to constraints.

Constraints must always be dealt with; they may be negotiable, though.

***Form***

Informal lists, structured by the sub-sections of this section.

***Examples***

see sub-sections

Background Information

In the optimal case constraints are defined by requirements. In any case, at least the architects must be aware of constraints.

The influence of constraints is described by [Hofmeister et al] (Software Architecture, A Practical Guide, Addison Wesley 1999) using the term “global analysis”.

## Technical Constraints

Contents

List all technical constraints in this section. This category covers hard- and software infrastructure, applied technologies (operating systems, middleware, databases, programming languages, …).

|  |  |
| --- | --- |
| Hardware-Constraints | |
|  | Hardware should be able to host an Operating System |
| Software-Constraints | |
|  | Binary compatibility of C++ libraries |
| Operating System Constraints | |
|  | Platform independent: Linux, Windows, Windows CE, QNX, VXWorks, ARM Linux |
| Programming Constraints | |
|  | Runtime should be done in C++, language for Trentino tool is free of choice |

Examples

|  |  |
| --- | --- |
| Constraint | Description |
| Hardware infrastructure | Processors, memory, networks, firewalls and other relevant elements |
| Software infrastructure | Operating systems, database systems, middleware, communications systems, transaction monitors, web servers, directory services |
| System operations | Batch- or online operations of the system or of required external systems? |
| Availability of the runtime environment | Data center with 7x24 uptime?  Will there be service times that cause reduced availability of the system or important parts thereof? |
| Graphical user interface | Are there any restrictions related to GUI (style guide)? |
| Libraries, frameworks, components | Is there any COTS that must be used? |
| Programming languages | Object oriented, structured, declarative, or rule-based languages?  Compiled or interpreted languages? |
| Reference architectures | Are there any comparable or reusable reference projects in the organization? |
| Analysis and design methodologies | Object oriented or structured methodologies? |
| Data structures | Requirements for certain data structures, interfaces to existing databases or files? |
| Software interfaces | Interfaces to existing applications |
| Programming requirements | Programming guidelines, fixed program structure |
| Technical communications | synchronous or asynchronous; protocols |

## Organizational Constraints

Contents

Enter all organizational, structural, and resource-related constraints. This category also covers standards and legal constraints that you must comply with.

|  |  |
| --- | --- |
| Organization and Structure | |
|  | Frequent changes of persons assigned to the project |
|  | Multi site development (China, Germany, Russia, Turkey) |
| Resources (Budget, Time, Personnel) | |
|  | Fixed number of 5 full time developers assigned |
| Organizational Standards | |
|  | OASIS SCA specification should be implemented |

Examples

| Constraint | Description |
| --- | --- |
| Organization and Structure | |
| Sponsor’s organizational structure | Potential changes of responsibilities?  Changes of contact persons? |
| Project team’s organizational structure | with/without subcontractors  decision-making power of the project manager |
| Decision makers | Experience with similar projects |
| Existing partnerships or co-operations | Are there any co-operations between the organizations and certain software companies?  Such partnerships often influence procurement decisions (independent of system requirements). |
| Internal development or outsourcing | Develop internally or outsource to external service companies? |
| Development of a product or for internal use? | Implies different processes in requirements analysis and decision making.  In the case of product development:  New product for a new market?  Improved product for an existing market?  Productizing of an existing (internal) system?  Development for internal use only? |
| Resources (Budget, Time, Personnel) | |
| Fixed price or time/effort? | Is the project’s budget fixed or is it calculated by time or effort? |
| Schedule | Is the schedule flexible? Is there a fixed delivery date? Which stakeholders control the delivery date? |
| Schedule vs. functionality | What has higher priority: The delivery date or the functionality? |
| Release-schedule | At which dates should which functionality be available in which releases / versions? |
| Project’s budget | Fixed or flexible? What amount is available? |
| Budget for technical resources | Buy or rent development tools? (hardware and software) |
| Team | Number of team members, qualifications, motivation, availability. |
| Organizational Standards | |
| Development process | Requirements concerning development process? This includes internal standards for modeling, documentation and implementation. |
| Quality standards | Is the organization required to adhere to quality standards (such as ISO-9000)? |
| Development tools | Requirements related to development tools (such as CASE-Tool, database, IDE, communications software, middleware, transaction monitor). |
| Configuration and version management | Requirements concerning processes and tools |
| Test tools and processes | Requirements concerning processes and tools |
| Acceptance- and release processes | Data modeling and database design  User interfaces  Business processes (workflow)  Usage of external systems (e.g. write access to external databases) |
| Service Level Agreements | Requirements or standards related to availability or required service levels? |
| Legal Factors | |
| Liability | Are there any legal aspects related to usage or operations of the system?  Could the system cause loss of human life or hazard to human health?  Could the system impact the operations of external systems or businesses? |
| Data privacy and security | Does the system store or process any data worthy of protection |
| Auditing | Are any aspects of the system under legal obligation to present evidence? |
| Aspects of international law | Will the system be used in an international context?  Are there varying constraints on system usage in different countries (example: use of encryption technology)? |

## Conventions

Contents

List all conventions that are relevant for the development of your software architecture.

Form

Either insert the conventions directly in this document or refer to other documents.

Examples

1. Coding guidelines
2. Documentation guidelines
3. Guidelines for version and configuration management
4. Naming conventions

# System Scope and Context

Contents

The context view defines the boundaries of the system under development to distinguish it from neighboring systems. It thereby identifies the system’s relevant external interfaces.

Make sure that the interfaces are specified with all their relevant aspects (what is communicated, in which format is it communicated, what is the transport medium, …), even though some popular diagrams (such as the UML use case diagram) represent only a few aspects of the interface.

Motivation

The interfaces to neighboring systems are among most critical and risky aspects of a project. Ensure early on that you have understood them in their entirety.

Form

1. Various context diagram (see below)
2. Lists of neighboring systems and their interfaces.

## Business Context

Contents

Identify all[[1]](#footnote-1) neighboring systems and specify all logical/business data that is exchanged with the system under development. Add data formats and communication protocols with neighboring systems and the general environment if these are not specified in detail with the relevant components.

Motivation

Understanding the information exchange with neighboring systems (i.e. all input flows and all output flows).

Form

Logical context diagram.

In UML this can be simulated e.g. by class diagrams, use case diagrams, communications diagrams – i.e. all diagrams that represent the system as a black box and explain its interfaces to neighboring systems (in varying degrees of detail).

If there are many neighboring systems you can substitute the context diagram with a table, including all the neighboring systems, their inputs and their outputs.

## Technical Context

Contents

Specification of the communication channels linking your system to neighboring systems and the environment.

Motivation

Understanding of the media used for information exchange with neighboring systems, and the environment.

Form

E.g. UML deployment diagram describing channels to neighboring systems, together with a mapping table of logical input and output flows of the logical context diagram (3.1) to the channels.

## External Interfaces

For many building blocks you can describe its interfaces directly in the black box template of the building block. For complex interfaces – and external interfaces are normally very complex – it is worth while to describe them in separate sections. Use the following interface template to guide you towards many questions that might be relevant for the interface.

#### Interface Id

|  |  |
| --- | --- |
| Name | <name of Interface> |
| Version |  |
| Changes w.r.t previous release |  |
| Who changed it and why? |  |
| Contact person |  |

#### Business Context of the Interface

#### Business Processes

<Diagram or desciption of business processes relevant for this interface>

#### Interface Data

<Description of interface data>

  Technical Context

  Form of interaction

#### Requirements for the Interface

#### Security Aspects

#### Quantities

   Runtime

   Throughput/Volume

  Availability

  Logging

  Archiving

#### Participating Resources

#### Syntax: Data and Formats

   Data Formats

   Validity & Plausibility Rules

   Encoding, Character Sets

   Configuration data

#### Syntax: Methods/Functions

  Check data

#### **Interface Process**

Logical and technical processes

#### Semantics

 Side effects, consequences

#### Technical Infrastructure

 Technical protocols

#### Error and Exception Handling

#### Constraints and Assumptions

 Access Rights

  Temporal constraints

  Parallel Access

  Preconditions for using the interface

#### Operating the Interface

#### Meta Information for the Interface

Person in charge

Costs of using the interface

Organizational Issues

Versioning

#### Examples of Using the Interface

Sample data

Sample flows and interactions

Programming Examples

### External Interface 1

<insert interface template>

### External Interface 2

<insert interface template>

### ...

### External Interface n

<insert interface template>

# Solution Strategy

Contents

A short summary and explanation of the fundamental solution ideas and strategies.

Motivation

An architecture is often based upon some key solution ideas or strategies. These ideas should be familiar to everyone involved into the architecture.

Form

Diagrams and / or text, as appropriate. Keep it short, i.e. 1 or 2 pages at most!

# Building Block View



Picture : Trentino building blocs

Trentino is composed of three main building blocs.

1. Trengen is the part of the platform that is in charge of validating SCA contribution before they are deployed into to Runtime. Trengen also perform code generation (e.g services proxies, stubs and skeletons, code to enable C++ reflection)
2. Trentino Runtime is the SCA container that hosts and runs SCA contributions.
3. The integration test framework simplify the task of creating integration tests for applications running on Trentino
4. The management and monitoring server is in charge of managing a set of contributions deployed on one or many devices.

Contents

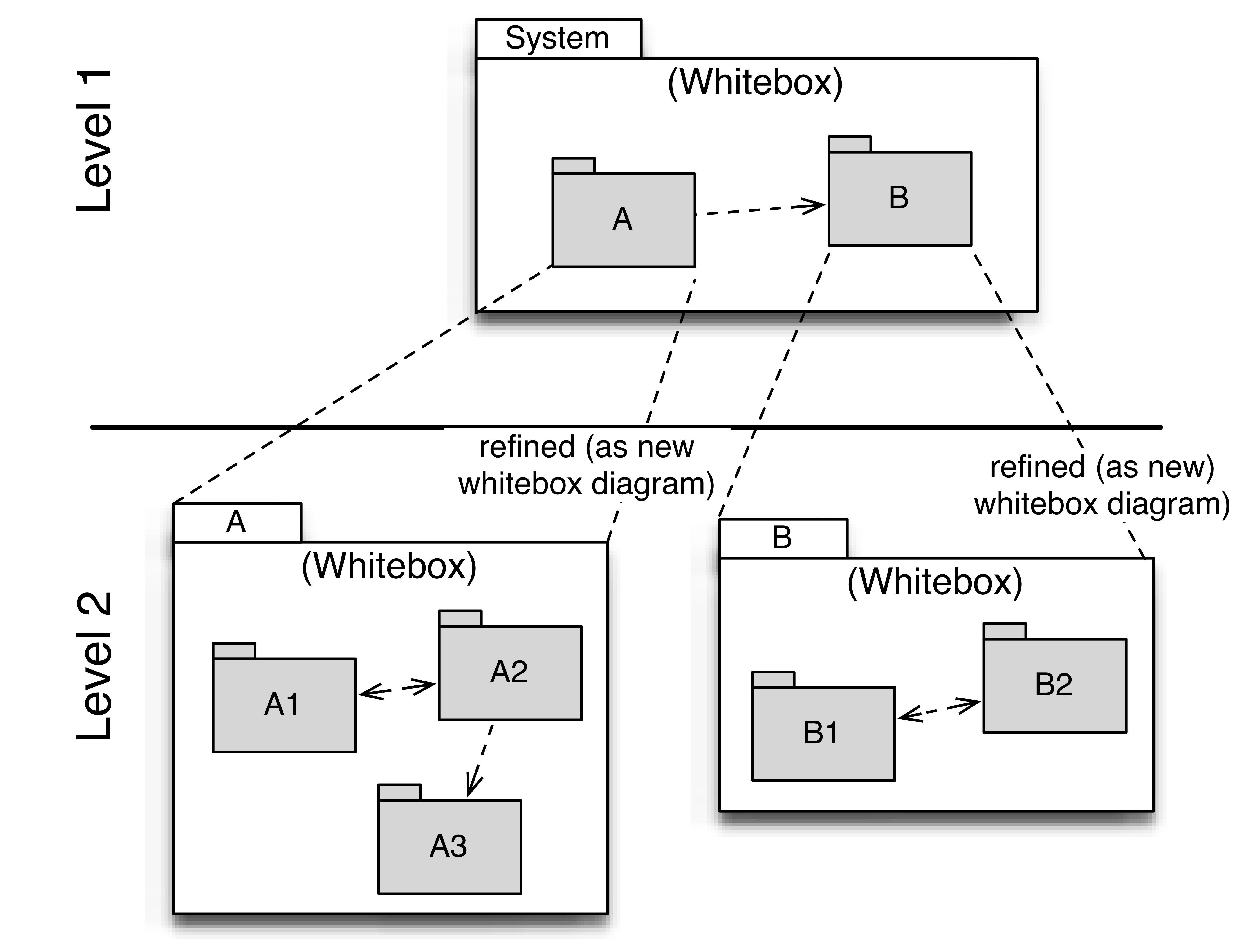
Static decomposition of the system into building blocks (modules, components, subsystems, subsidiary systems, classes, interfaces, packages, libraries, frameworks, layers, partitions, tiers, functions, macros, operations, data structures, …) and the relationships thereof.

Motivation

This is the most important view, that must be part of each architecture documentation. In building construction this would be the floor plan.

Form

The building block view is a hierarchical collection of black box and white box descriptions as shown in the following diagram:



Level 1 contains the white box description of the overall system (system under development / SUD) made up of black box descriptions of the system’s building blocks.

Level 2 zooms into the building blocks of Level 1 and is thus made up of the white box descriptions of all building blocks of Level 1 together with the black box descriptions of the building blocks of Level 2.

Level 3 zooms into the building blocks of Level 2, etc.

The section is structured as follows:

============================

White Box Template:

Contains multiple building blocks with corresponding black box descriptions.

One or more black box templates:

Each building block appearing in the white box template should be described as follows:

1. Purpose / Responsibility:
2. Interface(s):
3. Implemented requirements:
4. Variability:
5. Performance attributes:
6. Repository / Files:
7. Other administrative information: Author, Version, Date, Revision History
8. Open issues:

## Trentino Runtime

The runtime is the core of the platform, it executes SCA contributions as specified in the SCA Assembly model.



Picture 7: Trentino Building blocs

Trentino runtime is designed with extensibility in mind. Picture 7 shows a sketch of the layered functional architecture that supports the extensibility and ease of use for end-user developers.

Here you describe the white box view of level 1 according to the white box template. The structure is given below.

The overview diagram describes the inner structure of the overall system in terms of building blocks 1 – n, as well as their relationships and interdependencies.

It is also useful to list the most important reasons that led to this structure, esp. as relevant to the interdependencies / relationships among the building blocks at this level.

You should also mention rejected alternatives incl. reasons for their rejection.

### Runtime model

The Runtime model is the Trentino domain model; it contains descriptive information about a loaded SCA contribution / SCA composites and SCA components. The runtime is created by the contribution loader and is mainly read only for the other parts of the system. The runtime model use a generated SCA model that is a one to one mapping of the XML representation of a contribution.

#### SCA Model

The SCA Model is a C++ class representation of the information contained in SCDL language elements (based on the corresponding XML Schema) as well as in source code annotation for the SCA Assembly Model and the C++ Client and Implementation Model.

Hierarchical relations between entities in the SCA Spec are visible in the model.

The SCA Model is generated from the SCA Specification XML schema. The generation process is done in two steps:

### Bootsstrapper

The Bootstrapper start the Trentino runtime. It is in charge of:

1. Loading trentino extentions like Interception framework
2. Load plugged Binding frameworks
3. Creating the DomainContext as specified in the SCA SPEC
4. Creating the virtual Local Domain and the local domain composite
5. Instantiate management interface, so that remote console can connect to the runtime
6. Instantiate lifecycle manager and Registry and other Runtime components and connect them so that they can work together in one domain context
7. After the bootstrapper is instantiated, it delegates the start of deployed contributions to the lifecycle manager

The main entry point of the Bootstrapper is in the header file **cpp\src\Runtime\Core\TrentinoCoreBootstrappingRuntimeBootstrapper.h**

### Service invocation framework

The invocation framework is in charge of executing functions calls on given components.

It implements a responsibility chain / interceptor pattern used to perform aspect specific invocations before and after a method call. It is the place where exception handling.

The main components of the framework are:

1. SCA Policy and intent framework
2. Invoker

#### Trentino Invoker

The invoker is the entry point of a method of service invocation. The interface is located in file: **cpp\src\Runtime\Invocation\TrentinoInvocationInvokerBase.h**

##### Invoker interface

bool invoke(const Trentino::Invocation::InvocationData& data,

void\* retVal,

const Trentino::Invocation::InvocationContext& ctx) = 0;

Invoke is the main function provided by the invoker as parameters.

Input parameters:

1. are the invocation data, containing:
   1. The list of parameters of the method to be invoked
   2. The reference to the service to invoke
   3. The name of the method to invoke
2. A pointer to the returned value
3. An invocation context

The invoker is used by local services to access other local services. It is also used by remote services to access services.

##### Invoker threading

The current implementation of Trentino uses only one instance of the invoker for the whole runtime. The implementation should make sure that invoker is thread safe.

Structure according to black box template:

1. Purpose / Responsibility:
2. Interface(s):
3. Implemented requirements:
4. Variability:
5. Performance attributes:
6. Repository / Files:
7. Other administrative information: Author, Version, Date, Revision History
8. Open issues:

<insert the building block’s black box template here>

### Building Block Name 2 (Black Box Description)

<insert the building block’s black box template here>

### ...

<insert the building block’s black box template here>

### Building Block Name n (Black Box Description)

<insert the building block’s black box template here>

### Open Issues

## Level 2

Describe all building blocks comprising level 1 as a series of white box templates. The structure is given below for three building blocks and should be duplicated as needed.

### Building Block Name 1 (White Box Description)

Shows the inner workings of the building block in form of a diagrams with local building blocks 1 – n, as well as their relationships and interdependencies.

It is also useful to list the most important reasons that led to this structure, esp. as relevant to the interdependencies / relationships among the building blocks at this level.

You should also mention rejected alternatives incl. reasons for their rejection.

<insert diagram of building block 1 here>

#### Building Block Name 1.1 (Black Box Description)

Structure according to black box template:

1. Purpose / Responsibility:
2. Interface(s):
3. Implemented requirements:
4. Variability:
5. Performance attributes:
6. Repository / Files:
7. Other administrative information: Author, Version, Date, Revision History
8. Open issues:

#### Building Block Name 1.2 (Black Box Description)

Structure according to black box template

#### ...

#### Building Block Name 1.n (Black Box Description)

Structure according to black box template

#### Description of Relationships

#### Open Issues

### Building Block Name 2 (White Box Description)

…

<insert diagram of building block 2 here>

#### Building Block Name 2.1 (Black Box Description)

Structure according to black box template

#### Building Block Name 2.2 (Black Box Description)

Structure according to black box template

#### ...

#### Building Block Name 2.n (Black Box Description)

Structure according to black box template

#### Description of Relationships

#### Open Issues

### Building Block Name 3 (White Box Description)

…

<insert diagram of building block 3 here>

#### Building Block Name 3.1 (Black Box Description)

Structure according to black box template

#### Building Block Name 3.2 (Black Box Description)

Structure according to black box template

#### ...

#### Building Block Name 3.n (Black Box Description)

Structure according to black box template

#### Description of Relationships

#### Open Issues

## Level 3

Describe all building blocks comprising level 2 as a series of white box templates. The structure is identical to the structure of level 2. Duplicate the corresponding sub-sections as needed.

Simply use this section structure for any additional levels you would like to describe.

# Runtime View

Contents

alternative terms:

1. Dynamic view
2. Process view
3. Workflow view

This view describes the behavior and interaction of the system’s building blocks as runtime elements (processes, tasks, activities, threads, …).

Select interesting runtime scenarios such as:

1. How are the most important use cases executed by the architectural building blocks?
2. Which instances of architectural building blocks are created at runtime and how are they started, controlled, and stopped.
3. How do the system’s components co-operate with external and pre-existing components?
4. How is the system started (covering e.g. required start scripts, dependencies on external systems, databases, communications systems, etc.)?

Note: The main criterion for the choice of possible scenarios (sequences, workflows) is their *architectural relevancy*. It is not important to describe a large number of scenarios. You should rather document a representative selection.

Candidates are:

1. The top 3 – 5 use cases
2. System startup
3. The system’s behavior on its most important external interfaces
4. The system’s behavior in the most important error situations

Motivation

Esp. for object-oriented architectures it is not sufficient to specify the building blocks with their interfaces, but also how instances of building blocks interact during runtime.

Form

Document the chosen scenarios using UML sequence, activity or communications diagrams. Enumerated lists are sometimes feasible.

Using object diagrams you can depict snapshots of existing runtime objects as well as instantiated relationships. The UML allows to distinguish between active and passive objects.

## Runtime Scenario 1

1. Runtime diagram (or other adequate description of scenario!)
2. Description of the notable aspects of the interactions between the building block instances depicted in this diagram.

## Runtime Scenario 2

1. Runtime diagram (or other adequate description of scenario!)
2. Description of the notable aspects of the interactions between the building block instances depicted in this diagram.

## ...

## Runtime Scenario n

1. Runtime diagram (or other adequate description of scenario!)
2. Description of the notable aspects of the interactions between the building block instances depicted in this diagram.

# Deployment View

Contents

This view describes the environment within which the system is executed. It describes the geographic distribution of the system or the structure of the hardware components that execute the software. It documents workstations, processors, network topologies and channels, as well as other elements of the physical system environment. The deployment view shows the system from the operator’s point of view.

Please explain how the systems’ building blocks are aggregated or packaged into deployment artifacts or deployment units.

Motivation

Software is not much use without hardware. The minimum that is needed by you as a software architect is sufficient detail of the underlying (hardware) deployment so that you can assign each software building block that is relevant for the system’s operations to some hardware element. (This also holds for any COTS that is a prerequisite for the operations of the overall system.) These models should enable the operator to properly install the software.

Form

The UML provides deployment diagrams for describing this view. Use these – possibly in a nested manner if necessary. (The top level deployment diagram should already be part of your context view, showing your infrastructure as a single black box (cf. chapter 3.2). Here you are zooming into this black box with additional deployment diagrams.)

Diagrams by your hardware-oriented colleagues who describe processors and channels are also usable. You should abstract these to aspects relevant for software deployment.

## Infrastructure Level 1

### Deployment Diagram Level 1

1. Shows the deployment of the overall system to 1 – n processors or sites as well as the physical connections among these elements.
2. Lists the most important reasons that led to this deployment structure, i.e. the specific selection of nodes and channels.
3. Should also mention rejected alternatives incl. reasons for their rejection.

### Processor 1

< insert node template here>

node template:

* Description
* Deployed software building blocks
* Quality attributes (performance, constraints, ...)
* Other administrative information
* Open issues

### Processor 2

< insert node template here>

### ...

### Processor n

< insert node template here>

### Channel 1

Contents

Specification of the channel’s attributes, as relevant for software architecture.

Motivation

Specify at least those attributes of the communications channels that you need for proving fulfillment of non-functional requirements such as maximal throughput, probability for faults, etc.

Form

Often you will refer to a standard (e.g. CAN-Bus, 10Mbit Ethernet, IEEE 1394, ...).

If you need more information use a structure similar to the node template (especially to document quality aspects of channels like throughput, error rates, ...)

### Channel 2

### ...

### Channel m

## Infrastructure Level 2

Contents

Additional deployment diagrams with similar structure as above, refining each node of infrastructure level 1 that needs more details to map the software blocks.

Motivation

To describe additional details of the infrastructure, as needed by software deployment.

# Concepts

Contents

The following chapters cover examples of frequent cross-cutting concerns (a.k.a. aspects in some programming languages)

Fill in these chapters if there is NO building block that covers this aspect. If some of the concepts are not relevant for your project mention this fact instead of removing the section.

Motivation

Some concept cannot be “factored” into a separate building block of the architecture (e.g. the topic “security”). This section of the template is the location where you can describe all decision for such a cross cutting topic in one central place. Nevertheless, you have to make sure that all your building blocks conform to such decisions.

Form

.. can be varied. Some concepts are plain natural language text with a freely chosen structure, some others may include models/scenarios using notations that are also applied in architecture views.

## Domain Models

Contents

Business (or logical) models, domain models - they all describe subject-specific, business aspects, without relation to technology.

Often these structures or concepts are re-used at many places within an architecture, especially within chapter [5. Building Block View](http://confluence.arc42.org/display/templateEN/5.+Building+Block+View)..

Motivation

Often parts of these models reappear in the building block view, but in order to „keep them clean from technnology“ they can be captured as a concept.

Form

Usually either ER-Models (Entity-Relationship Models) or UML class diagrams (mainly containing entity classes) are used to document domain models.

## Recurring or Generic Structures and Patterns

Motivation

Sometimes a hierarchical decomposition of building blocks is insufficient for giving an overview of detailed interdependencies between individual building blocks. The following sections are intended to describe generic or specific dependencies among any set of building blocks – possibly even across different levels.

We call a dependency *generic* if it appears more than once in the architecture, and *specific* if it is unique.

Form

Use building block models (class diagrams, package diagrams, component diagrams, etc.) and related descriptions in the same way as in the hierarchical decomposition.

Often it is practical to support understandability by adding specific runtime views to explain these recurring structures.

### Recurring or Generic Structure 1

<insert diagram and descriptions here>

### Recurring or Generic Structure 2

<insert diagram and descriptions here>

## Persistency

Persistency means moving data from (volatile) memory to a durable storage medium (and back).

Some of the data that a software system is processing must be written to and read from persistent storage media.

1. Volatile storage media (main memory or cache) are not designed for permanent storage. Data is lost if the hardware is switched off.
2. The amount of data processed by commercial software systems normally exceeds the capacity of main memory.
3. Hard disks, optical media and tapes often contain large amounts of existing business data that represent a significant investment.

Persistency is a technical issue that normally does not appear as part of the actual business functionality. An architect must deal with this issue nevertheless because most software systems require efficient access to persistently stored data. This is relevant for essentially all commercial and most technical systems; embedded systems on the other hand often differ in their data management requirements.

## User Interface

Software systems that are used interactively by (human) users require a user interface. These can be graphical, textual, or voice user interfaces.

## Ergonomics

Ergonomics of software systems deals with the improvement (optimization) of their usability with respect to objective and subjective factors. Key ergonomic factors are user interface, reactivity (subjective performance) as well as availability and robustness of the system.

## Flow of Control

Flow of control for software systems is related to visible flows (on the - graphical - user interface) as well as the flow of background activities. Therefore this section should cover control of the user interface as well as control of workflows.

## Transaction Procession

A transaction is a sets of operations or activities that must be processed either in its entirety or not at all. The term is especially relevant in the database area with the important notion of ACID-transactions (atomic, consistent, isolated, durable).

## Session Handling

A session identifies an active connection between a client and a server. The session state must be preserved, which is esp. important if stateless protocols such as HTTP are used for communications. Session handling is a critical challenge esp. for intra- and internet-systems and can strongly influence the performance of a system.

## Security

The security of software systems deals with mechanisms that ensure data confidentiality, integrity, and availability.

Typical issues are:

1. How can data be protected during transport (e.g. via open networks such as the internet)?
2. How can communicating entities ensure mutual trust?
3. How can communicating entities identify each other and be protected against faked identities?
4. How can communicating entities prove data provenience or certify validity of data?

The topic of IT-security often touches upon legal aspects, sometimes even international law.

## Safety

The safety of software systems deals with mechanisms that ensure that human life or our environment is not endangered.

Describe your concept here: identify those parts of the system that might endanger life and describe mechanism to ensure proper safety.

## Communications and Integration

Communication: Exchange of data between system components. Covers communications within one process or address space, between different processes (inter-process communication – IPC), and between different systems.

Integration: Combination of existing systems in a new context. Also known as: (Legacy) Wrapper, Gateway, Enterprise Application Integration (EAI).

## Distribution

Distribution: Design of software systems whose parts are executed on different – physically separated – hardware systems.

Distribution covers issues such as calling methods on remote systems (remote procedure call – RPC or remote method invocation – RMI), the transfer of data or documents among distributed parties, the choice of optimal modes of interaction or communications patterns (such as synchronous / asynchronous, publish-subscribe, peer-to-peer).

## Plausibility and Validity Checks

How and where do you check plausibility and validity of (input) data, esp. user inputs?

## Exception/Error Handling

How are exceptions and errors handled systematically and consistently?

How can the system reach a consistent state after an error? Is this done automatically or is manual interaction required?

This aspect is also related to logging and tracing,

Which kind of exceptions and errors are handled by the system? Which kinds of errors are forwarded to which external interface and which are handled fully internally?

How do you use the exception handling mechanisms of your programming language? Do you use checked or unchecked exceptions?

## System Management and Administration

Larger software systems are often executed in controlled environments (data centers) under oversight of operators or administrators. These stakeholders require specific information on the applications’ states during runtime as well as special means of control and configuration.

## Logging, Tracing

There are two ways of documenting an application’s status during runtime: *Logging* and *Tracing*. In both cases the application is extended with function or method calls that write state information, but there is a difference in their usage:

1. Logging can cover business or technical aspects or any combination of both.
2. Business logs are normally prepared for end users, administrators or operators. They contain information on the business processes that are executed by the application. This kind of logging may also be related to auditing.
3. Technical logs contain information for operators or developers. These are used for error detection and system optimization.
4. Tracing is intended to provide debugging information for developers or support personnel. It is primarily used for error detection and analysis.

## Business Rules

How do you deal with business logic and business rules? Is business logic implemented in the corresponding business classes or is it handled in a central component? Do you use a rule engine for the interpretation of business rules (production system, forward-/backward-chaining)?

## Configurability

The flexibility of a software system is influenced by its configurability, i.e. the possibility to make certain decisions about usage of the system at a late point in time.

Configurability can occur at the following events:

1. During development: For example server, file, or directory names could be stored directly in the code (“hard-coded”).
2. During deployment or installation: Configuration information for a specific installation (such as the installation path) can be given.
3. At system startup: Information can be read dynamically before or during system startup.
4. During application execution: Configuration information is queried or read during runtime.

## Parallelization and Threading

Applications can be executed in parallel processes or threads. This creates a need for synchronization points. The theory of parallel processing serves as a foundation for this aspect. The architecture and implementation of parallel systems needs to consider many technical details such as address spaces, applied mechanisms for synchronization – guards, semaphores, etc. – processes and threads, parallelism in the operating system, parallelism in virtual machines. etc.

## Internationalization

This section covers support for usage of the system in different countries, i.e. adjusting the system to country specific attributes. Internationalization (often abbreviated as “i18n” where “18” refers to the eighteen characters between the I and the n) covers translation of text, usage of character encodings, display of fonts, writing of numbers and dates, and other (external) aspects.

## Migration

In many cases a new software system is intended to replace an existing legacy system. As an architect you should not only consider your shiny new architecture but also all organizational and technical aspects that must be considered for the introduction or migration of the architecture.

Examples:

1. Concept, process, or tools for data transfer and initial data creation.
2. Concept for system introduction or temporary parallel operations of legacy system and new system.

Is it necessary to migrate existing data? How do you execute any needed syntactic or semantic transformations?

## Testability

Support for simple (and if possible automated) tests. This aspect is the basis for the important implementation pattern of “continuous integration”. Projects should support at least daily build-and-test cycles. Important keywords for this aspect are unit tests and mock objects.

## Scaling, Clustering

How can your system grow in a way that can cope with more load or a larger number of users and still keep up performance and throughput.

## High Availability

How can you achieve high availability of your system? Do you use redundancy of major parts? Or do you distribute your system to different processors or locations. Are you running standby- systems?

## Code Generation

How and where do you use code generators to create parts of the system from models or domain specific languages (DSL’s)?

## Build-Management

How is the overall system created from is (source code) building blocks? Which repositories contain source code, where are configuration files, test cases, test data and build scripts (make, ant, maven) stored?

# Design Decisions

Contents

Document all important design decisions and their reasons!

Motivation

It is advantageous if all important design decisions can be found in one place. It is up to you to decide if a decision should be documented here or rather locally (e.g. in the white box descriptions of building blocks). In any case avoid redundancies.

Form

Informal list, if possible ordered by the decisions’ importance for the reader. Use the following template to structure your decisions.

**9.x.1 Problem**

What exactly is the challenge?

Why is it relevant for the architecture?

What consequences does the decision have?

**9.x.2 Constraints**

Which constraints do you have to keep in mind?

What factors influence the decision?

**9.x.3 Assumptions**

Which assumption have you made?

How can you check those assumptions?

Which risks are you facing?

**9.x.4 Considered Alternatives**

Which alternative options did you consider?

How do you judge each one?

Which alternatives are you excluding deliberately?

**9.x.5 Decision**

Who (if not you) has decided?

How has the decision been justified?

When did you decide?

## <Decision Topic 1>

## <Decision Topic 2>

## <Decision Topic 3>

## ...

# Quality Scenarios

This chapter summarizes all you (or other stakeholders) might need to systematically evaluate the architecture against the quality requirements.

It contains:

* Quality Tree (sometimes called utility tree), an overview of the quality requirements
* Evaluation or quality scenarios - detailed descriptions of the quality requirements or goals.

## Quality Tree

Content

The quality tree ( as defined in ATAM – Architecture Tradeoff Analysis Method) with quality / evaluation scenarios as leafs.

Motivation

When you want to evaluate the quality (especially risks to certain quality attributes) with methods like ATAM, you need to systematically refine your quality goals (from chapter 1.2). The quality tree shows the top-down refinement of the stakeholder-specific notion of quality.

Form

We personally prefer mind maps to a pure tree-like structure, as mind maps allow arbitrary cross-references between scenarios, attributes and intermediate nodes.

Often it is difficult to assign scenarios to single quality attributes, as the scenario refers to several qualities at once. Simply draw references from such scenarios to all affected nodes!

## Evaluation Scenarios

Contents

Scenarios describe a system’s reaction to a stimulus in a certain situation. They thus characterize the interaction between stakeholders and the system. Scenarios operationalize quality criteria and turn them into measurable quantities.

Two scenarios are relevant for most software architects:

1. Usage scenarios (also called application scenarios or use case scenarios) the system’s runtime reaction to a certain stimulus. This also includes scenarios that describe the system’s efficiency or performance. Example: The system reacts to a user’s request within one second.
2. Change scenarios describe a modification of the system or of its immediate environment. Example: Additional functionality is implemented or requirements for a quality attribute change.

If you design safety critical systems a third type of scenarios is important for you:

1. Boundary or stress scenarios describe how the system reacts to exceptional conditions. Examples: How does the system react to a complete power outage, a serious hardware failure, etc.

**Source of**

**the Stimulus**

**System**

**artifact**

**Response measure**

**Stimulus**

**Response**

**Figure: Schematic depiction of scenarios (cf. [Bass+03])**

Scenarios comprise the following major parts (according to [Starke05], original structure from [Bass+03]):

1. Stimulus: Describes a specific interaction between the (stimulating) stakeholder and the system. Example: A user calls a functions, a developer implements an extension, an administrator installs or configures the system.
2. Source of the stimulus: Describes where the stimulus comes from. Examples: internal or external, user, operator, attacker, manager.
3. Environment: Describes the system’s state at the time of arrival of the stimulus. This should list all preconditions that are necessary for comprehension of the scenario. Examples: Is the system under normal or maximal load? Is the data base available or down? Are any users online?
4. System artifact: Describes the part of the system is affected by the stimulus. Examples: The whole system, the data base, the web server.
5. System response: Describes the system’s reaction to the stimulus as determined by the architecture. Examples: Is the function called by the user executed. How long does the developer need for implementation? Which parts of the system are affected by the installation / configuration?
6. Response measure: Describes how the response can be measured or evaluated. Examples: Downtime in hours, correctness yes/no, time for code change in person days, reaction time in seconds.

Motivation

You need scenarios for the evaluation and review of architectures. They take the role of a “benchmark” and aid in measuring the architecture’s achievement of its objectives regarding the non-functional requirements and quality attributes.

Form

Tabular or free text. Explicitly highlight the scenario’s elements (source, environment, artifact, response, measure).

Alternatively, use similar notations as those suggested in [6. Runtime View](http://arc42.org:8090/display/templateEN/6.+Runtime+View).

Background Information

There are relations between scenarios and the runtime view. Often you can use scenarios of the runtime view fully or as a basis for evaluation. Evaluation scenarios additionally contain response measures that are often not considered in the pure execution focus of runtime scenarios.

# Technical Risks

Contents

A list of identified technical risks, ordered by priority

Motivation

“Risk management is project management for grown-ups” (Tim Lister, Atlantic Systems Guild.) This should be your motto for systematic detection and evaluation of technical risks in the architecture, which will be needed by project management as part of the overall risk analysis.

Form

List of risks with probability of occurrence, amount of damage, options for risk avoidance or risk mitigation, …

# Glossary

Contents

The most important terms of the software architecture in alphabetic order.

Motivation

It should not be necessary to explain the usefulness of a glossary …

Form

A simple table with columns <Term> and <Definition>

1. We often tend to a pragmatic approach – but here we insist on a list of all (a-l-l) neighboring systems. Too many projects have failed because they were not aware of their neighbors. ☹ [↑](#footnote-ref-1)