fly

www.nasa.gov

integrate

NASA SYSTEMS ENGINEERING HANDBOOK

design

National Aeronautics and Space Administration

test

NASA SP-2016-6105 Rev2 supersedes SP-2007-6105 Rev 1 dated December, 2007.

Cover photos: *Top left:* In this photo, engineers led by researcher Greg Gatlin have sprayed fluorescent oil on a 5.8 percent scale model of a futuristic hybrid wing body during tests in the 14- by 22-Foot Subsonic Wind Tunnel at NASA’s Langley Research Center in Hampton, VA. The oil helps researchers “see” the flow patterns when air passes over and around the model. (NASA Langley/ Preston Martin) *Top right:* Water impact test of a test version of the Orion spacecraft took place on August 24, 2016, at NASA Langley Research Center (NASA) *Bottom left:* two test mirror segments are placed onto the support structure that will hold them. (NASA/Chris Gunn) *Bottom right:* This self-portrait of NASA’s Curiosity Mars rover shows the vehicle at the “Mojave” site, where its drill collected the mission’s second taste of Mount Sharp. (NASA/JPL-Caltech/MSSS)

Comments, questions, and suggestions regarding this document can be sent to:

Steven R. Hirshorn Chief Engineer, Aeronautics Research Mission Directorate (ARMD) Office of the Chief Engineer NASA Headquarters, Room 6D37 300 E St SW Washington, DC 20546-0001 202-358-0775 *steven.r.hirshorn@nasa.gov*

Table of Contents

*Preface viii*

*Acknowledgments ix*

1.0 Introduction 1

1.1 Purpose . . . . . . . . . . . . . . . . 1 1.2 Scope and Depth . . . . . . . . . . . 1

2.0 Fundamentals of Systems Engineering 3

2.1 The Common Technical Processes

and the SE Engine . . . . . . . . . . . 5 2.2 An Overview of the SE Engine by

Project Phase . . . . . . . . . . . . . 8 2.3 Example of Using the SE Engine . . . . 10 2.4 Distinctions between Product

Verification and Product Validation . . . 11 2.5 Cost Effectiveness Considerations . . . 11 2.6 Human Systems Integration (HSI)

in the SE Process . . . . . . . . . . .12 2.7 Competency Model for

Systems Engineers . . . . . . . . . . . 13

3.0 NASA Program/Project Life Cycle 17

3.1 Program Formulation . . . . . . . . . .20 3.2 Program Implementation . . . . . . . . 20 3.3 Project Pre-Phase A: Concept Studies . 21 3.4 Project Phase A: Concept and

Technology Development . . . . . . . .23 3.5 Project Phase B: Preliminary Design

and Technology Completion . . . . . . 25 3.6 Project Phase C: Final Design and

Fabrication . . . . . . . . . . . . . . . 27 3.7 Project Phase D: System Assembly,

Integration and Test, Launch . . . . . . 29 3.8 Project Phase E: Operations

and Sustainment . . . . . . . . . . . . 31 3.9 Project Phase F: Closeout . . . . . . . 31

3.10 Funding: The Budget Cycle . . . . . . . 33 3.11 Tailoring and Customization of

NPR 7123 .1 Requirements . . . . . . . 34 3.11.1 *Introduction 34* 3.11.2 *Criteria for Tailoring 34* 3.11.3 *Tailoring SE NPR Requirements*

*Using the Compliance Matrix 35*

3.11.4 *Ways to Tailor a SE Requirement 36* 3.11.5 *Examples of Tailoring and Customization 37*

3.11.6 *Approvals for Tailoring 40*

4.0 System Design Processes 43

4.1 Stakeholder Expectations Definition . . 45

4.1.1 *Process Description 45* 4.1.2 *Stakeholder Expectations Definition*

*Guidance 53* 4.2 Technical Requirements Definition . . . 54

4.2.1 *Process Description 54* 4.2.2 *Technical Requirements Definition*

*Guidance 62* 4.3 Logical Decomposition . . . . . . . . .62

4.3.1 *Process Description 62* 4.3.2 *Logical Decomposition Guidance 65* 4.4 Design Solution Definition . . . . . . .65

4.4.1 *Process Description 66* 4.4.2 *Design Solution Definition Guidance 76*

5.0 Product Realization 77

5.1 Product Implementation . . . . . . . . 78

5.1.1 *Process Description 79* 5.1.2 *Product Implementation Guidance 83* 5.2 Product Integration . . . . . . . . . . .83

5.2.1 *Process Description 85* 5.2.2 *Product Integration Guidance 88* 5.3 Product Verification . . . . . . . . . . .88

iii NASA SYSTEMS ENGINEERING HANDBOOK

Table of Contents

5.3.1 *Process Description 89* 5.3.2 *Product Verification Guidance 99* 5.4 Product Validation . . . . . . . . . . .99

5.4.1 *Process Description 99* 5.4.2 *Product Validation Guidance 106* 5.5 Product Transition . . . . . . . . . . 106

5.5.1 *Process Description 106* 5.5.2 *Product Transition Guidance 112*

6.0 Crosscutting Technical Management 113

6.1 Technical Planning . . . . . . . . . . 113

6.1.1 *Process Description 114* 6.1.2 *Technical Planning Guidance 130* 6.2 Requirements Management . . . . . 130

6.2.1 *Process Description 131* 6.2.2 *Requirements Management*

*Guidance 135* 6.3 Interface Management . . . . . . . . 135

6.3.1 *Process Description 136* 6.3.2 *Interface Management Guidance 138* 6.4 Technical Risk Management . . . . . 138

6.4.1 *Risk Management Process*

*Description 141*

6.4.2 *Risk Management Process*

*Guidance 143* 6.5 Configuration Management . . . . . . 143

6.5.1 *Process Description 144* 6.5.2 *CM Guidance 150* 6.6 Technical Data Management . . . . . 151

6.6.1 *Process Description 151* 6.6.2 *Technical Data Management*

*Guidance 155* 6.7 Technical Assessment . . . . . . . . 155

6.7.1 *Process Description 157* 6.7.2 *Technical Assessment Guidance 160* 6.8 Decision Analysis . . . . . . . . . . . 160

6.8.1 *Process Description 164* 6.8.2 *Decision Analysis Guidance 170*

Appendix A Acronyms . . . . . . . . . . . . . . 173 Appendix B Glossary . . . . . . . . . . . . . . . 176 Appendix C How to Write a Good Requirement—

Checklist . . . . . . . . . . . . . . . 197 Appendix D Requirements Verification Matrix . . . 201 Appendix E Creating the Validation Plan with a

Validation Requirements Matrix . . . . 203 Appendix F Functional, Timing, and State Analysis 205 Appendix G Technology Assessment/Insertion . . 206 Appendix H Integration Plan Outline . . . . . . . . 214 Appendix I Verification and Validation Plan Outline 216 Appendix J SEMP Content Outline . . . . . . . . 223 Appendix K Technical Plans . . . . . . . . . . . . 235 Appendix L Interface Requirements Document

Outline . . . . . . . . . . . . . . . . 236 Appendix M CM Plan Outline . . . . . . . . . . . 239 Appendix N Guidance on Technical Peer

Reviews/Inspections . . . . . . . . . 240 Appendix O Reserved . . . . . . . . . . . . . . . 241 Appendix P SOW Review Checklist . . . . . . . . 242 Appendix Q Reserved . . . . . . . . . . . . . . . 243 Appendix R HSI Plan Content Outline . . . . . . . 244 Appendix S Concept of Operations

Annotated Outline . . . . . . . . . . 251 Appendix T Systems Engineering in Phase E . . . 254

*References Cited 260 Bibliography 270*

iv NASA SYSTEMS ENGINEERING HANDBOOK

Table of Figures

Figure 2.0-1 SE in Context of Overall Project

Management . . . . . . . . . . . . . 5 Figure 2.1-1 The Systems Engineering Engine

(NPR 7123 .1) . . . . . . . . . . . . . 6 Figure 2.2-1 Miniature Version of the Poster-Size

NASA Project Life Cycle Process Flow for Flight and Ground Systems Accompanying this Handbook . . . . 8 Figure 2.5-1 Life-Cycle Cost Impacts from Early

Phase Decision-Making . . . . . . . . 13 Figure 3.0-1 NASA Space Flight Project Life Cycle

from NPR 7120 .5E . . . . . . . . . . 18 Figure 3.11-1 Notional Space Flight Products

Tailoring Process . . . . . . . . . . .36 Figure 4.0-1 Interrelationships among the System

Design Processes . . . . . . . . . . .44 Figure 4.1-1 Stakeholder Expectations Definition

Process . . . . . . . . . . . . . . . .46 Figure 4.1-2 Information Flow for Stakeholder

Expectations . . . . . . . . . . . . .48 Figure 4.1-3 Example of a Lunar Sortie DRM Early in

the Life Cycle . . . . . . . . . . . . . 51 Figure 4.2-1 Technical Requirements Definition

Process . . . . . . . . . . . . . . . .55 Figure 4.2-2 Flow, Type and Ownership of

Requirements . . . . . . . . . . . . . 57 Figure 4.2-3 The Flowdown of Requirements . . . . 58 Figure 4.3-1 Logical Decomposition Process . . . . 63 Figure 4.4-1 Design Solution Definition Process . . 66 Figure 4.4-2 The Doctrine of Successive

Refinement . . . . . . . . . . . . . . 67 Figure 4.4-3 A Quantitative Objective Function,

Dependent on Life Cycle Cost and All Aspects of Effectiveness . . . . . . 71 Figure 5.0-1 Product Realization . . . . . . . . . . 78 Figure 5.1-1 Product Implementation Process . . . 79

Figure 5.2-1 Product Integration Process . . . . .86 Figure 5.3-1 Product Verification Process . . . . . 91 Figure 5.3-2 Example of End-to-End Data Flow

for a Scientific Satellite Mission . . . . 96 Figure 5.4-1 Product Validation Process . . . . . 100 Figure 5.5-1 Product Transition Process . . . . . 107 Figure 6.1-1 Technical Planning Process . . . . . 115 Figure 6.2-1 Requirements Management Process 131 Figure 6.3-1 Interface Management Process . . . 136 Figure 6.4-1 Risk Scenario Development . . . . . 139 Figure 6.4-2 Risk as an Aggregate Set of

Risk Triplets . . . . . . . . . . . . . 139 Figure 6.4-3 Risk Management Process . . . . . 141 Figure 6.4-4 Risk Management as the Interaction

of Risk-Informed Decision Making and Continuous Risk Management . 142 Figure 6.5-1 Configuration Management Process 145 Figure 6.5-2 Five Elements of Configuration

Management . . . . . . . . . . . . 145 Figure 6.5-3 Evolution of Technical Baseline . . . 147 Figure 6.5-4 Typical Change Control Process . . 148 Figure 6.6-1 Technical Data Management

Process . . . . . . . . . . . . . . . 151 Figure 6.7-1 Technical Assessment Process . . . 158 Figure 6.7-2 Planning and Status

Reporting Feedback Loop . . . . . 159 Figure 6.8-1 Decision Analysis Process . . . . . 165 Figure 6.8-2 Risk Analysis of Decision Alternatives 166 Figure G.1-1 PBS Example . . . . . . . . . . . . 208 Figure G.3-1 Technology Assessment Process . . 209 Figure G.3-2 Architectural Studies and

Technology Development . . . . . . 210 Figure G.4-1 Technology Readiness Levels . . . . 211 Figure G.4-2 TMA Thought Process . . . . . . . 212 Figure G.4-3 TRL Assessment Matrix . . . . . . . 213

v NASA SYSTEMS ENGINEERING HANDBOOK

Table of Tables

Table 2.1-1 Alignment of the 17 SE Processes to

AS9100 . . . . . . . . . . . . . . . . 7 Table 2.2-1 Project Life Cycle Phases . . . . . . . 9 Table 2.7-1 NASA System Engineering

Competency Model . . . . . . . . . . 14 Table 3.0-1 SE Product Maturity from NPR 7123 .1 19 Table 3.11-1 Example of Program/Project Types . . 38 Table 3.11-2 Example of Tailoring NPR 7120 .5

Required Project Products . . . . . .39 Table 3.11-3 Example Use of a Compliance Matrix . 41 Table 4.1-1 Stakeholder Identification

throughout the Life Cycle . . . . . . . 47 Table 4.2-1 Benefits of Well-Written Requirements 59 Table 4.2-2 Requirements Metadata . . . . . . .59 Table 5.3-1 Example information in Verification

Procedures and Reports . . . . . . .94 Table 6.1-1 Example Engineering Team

Disciplines in Pre-Phase A for Robotic Infrared Observatory . . . . 118

Table 6.1-2 Examples of Types of Facilities to

Consider during Planning . . . . . . 120 Table 6.6-1 Technical Data Tasks . . . . . . . . 156 Table 6.7-1 Purpose and Results for Life-Cycle

Reviews for Spaceflight Projects . . 161 Table 6.8-1 Typical Information to Capture in a

Decision Report . . . . . . . . . . . 171 Table D-1 Requirements Verification Matrix . . 202 Table E-1 Validation Requirements Matrix . . . 204 Table G.1-1 Products Provided by the TA as a

Function of Program/Project Phase . 207 Table J-1 Guidance on SEMP Content per

Life-Cycle Phase . . . . . . . . . . 233 Table K-1 Example of Expected Maturity of

Key Technical Plans . . . . . . . . . 235 Table R.2-1 HSI Activity, Product, or Risk Mitigation

by Program/Project Phase . . . . . 250

vi NASA SYSTEMS ENGINEERING HANDBOOK

Table of Boxes

The Systems Engineer’s Dilemma . . . . . . . . . . 12 Space Flight Program Formulation . . . . . . . . . . 20 Space Flight Program Implementation . . . . . . . . 21 Space Flight Pre-Phase A: Concept Studies . . . . . 22 Space Flight Phase A: Concept and Technology Development . . . . . . . 24 Space Flight Phase B: Preliminary Design and Technology Completion . . . 26 Space Flight Phase C: Final Design and Fabrication . 28 Space Flight Phase D: System Assembly, Integration and Test, Launch . . . 30 Space Flight Phase E: Operations and Sustainment . 32 Phase F: Closeout . . . . . . . . . . . . . . . . . .33 System Design Keys . . . . . . . . . . . . . . . . .44 Concept of Operations vs . Operations Concept . . . 51 Example of Functional and Performance Requirements . . . . . . . . . . . . . . . . . . . .56 Rationale . . . . . . . . . . . . . . . . . . . . . . .60 Product Realization Keys . . . . . . . . . . . . . . . 78

Differences between Verification and Validation Testing . . . . . . . . . . . . . . . . . . .89 Differences between Verification, Qualification, Acceptance and Certification . . . . . . . . . . . . .90 Methods of Verification . . . . . . . . . . . . . . . .93 Methods of Validation . . . . . . . . . . . . . . . 101 Crosscutting Technical Management Keys . . . . . 114 Types of Hardware . . . . . . . . . . . . . . . . . 124 Environments . . . . . . . . . . . . . . . . . . . . 127 Definitions . . . . . . . . . . . . . . . . . . . . . 130 Types of Configuration Management Changes . . . 149 Data Collection Checklist . . . . . . . . . . . . . . 155 HSI Relevance . . . . . . . . . . . . . . . . . . . 246 HSI Strategy . . . . . . . . . . . . . . . . . . . . 246 HSI Domains . . . . . . . . . . . . . . . . . . . . 247 HSI Requirements . . . . . . . . . . . . . . . . . 247 HSI Implementation . . . . . . . . . . . . . . . . 249 HSI Plan Updates . . . . . . . . . . . . . . . . . 250

vii NASA SYSTEMS ENGINEERING HANDBOOK

Preface

Since the initial writing of NASA/SP-6105 in 1995 and the following revision (Rev 1) in 2007, systems engineering as a discipline at the National Aeronautics and Space Administration (NASA) has undergone rapid and continued evolution. Changes include using Model-Based Systems Engineering to improve development and delivery of products, and accommo- dating updates to NASA Procedural Requirements (NPR) 7123.1. Lessons learned on systems engi- neering were documented in reports such as those by the NASA Integrated Action Team (NIAT), the Columbia Accident Investigation Board (CAIB), and the follow-on Diaz Report. Other lessons learned were garnered from the robotic missions such as Genesis and the Mars Reconnaissance Orbiter as well as from mishaps from ground operations and the commercial space flight industry. Out of these reports came the NASA Office of the Chief Engineer (OCE) initia- tive to improve the overall Agency systems engineer- ing infrastructure and capability for the efficient and effective engineering of NASA systems, to produce quality products, and to achieve mission success. This handbook update is a part of that OCE-sponsored Agency-wide systems engineering initiative.

In 1995, SP-6105 was initially published to bring the fundamental concepts and techniques of systems engi- neering to NASA personnel in a way that recognized the nature of NASA systems and the NASA environ- ment. This revision (Rev 2) of SP-6105 maintains that original philosophy while updating the Agency’s sys- tems engineering body of knowledge, providing guid- ance for insight into current best Agency practices, and maintaining the alignment of the handbook with the Agency’s systems engineering policy.

The update of this handbook continues the methodol- ogy of the previous revision: a top-down compatibility with higher level Agency policy and a bottom-up infu- sion of guidance from the NASA practitioners in the field. This approach provides the opportunity to obtain best practices from across NASA and bridge the infor- mation to the established NASA systems engineering processes and to communicate principles of good prac- tice as well as alternative approaches rather than spec- ify a particular way to accomplish a task. The result embodied in this handbook is a top-level implemen- tation approach on the practice of systems engineer- ing unique to NASA. Material used for updating this handbook has been drawn from many sources, includ- ing NPRs, Center systems engineering handbooks and processes, other Agency best practices, and external systems engineering textbooks and guides.

This handbook consists of six chapters: (1) an intro- duction, (2) a systems engineering fundamentals dis- cussion, (3) the NASA program/project life cycles, (4) systems engineering processes to get from a con- cept to a design, (5) systems engineering processes to get from a design to a final product, and (6) crosscut- ting management processes in systems engineering. The chapters are supplemented by appendices that provide outlines, examples, and further information to illustrate topics in the chapters. The handbook makes extensive use of boxes and figures to define, refine, illustrate, and extend concepts in the chapters.

Finally, it should be noted that this handbook provides top-level guidance for good systems engineering prac- tices; it is not intended in any way to be a directive.

NASA/SP-2016-6105 Rev2 supersedes SP-2007-6105 Rev 1 dated December, 2007.

viii NASA SYSTEMS ENGINEERING HANDBOOK

Acknowledgments

The following individuals are recognized as contrib- uting practitioners to the content of this expanded guidance:

Alexander, Michael, NASA/Langley Research Center

Allen, Martha, NASA/Marshall Space Flight Center

Baumann, Ethan, NASA/Armstrong Flight Research Center

Bixby, CJ, NASA/Armstrong Flight Research Center

Boland, Brian, NASA/Langley Research Center

Brady, Timothy, NASA/NASA Engineering and Safety Center

Bromley, Linda, NASA/Headquarters/Bromley SE Consulting

Brown, Mark, NASA/Jet Propulsion Laboratory

Brumfield, Mark, NASA/Goddard Space Flight Center

Campbell, Paul, NASA/Johnson Space Center

Carek, David, NASA/Glenn Research Center

Cox, Renee, NASA/Marshall Space Flight Center

Crable, Vicki, NASA/Glenn Research Center

Crocker, Alan, NASA/Ames Research Center

DeLoof, Richard, NASA/Glenn Research Center

Demo, Andrew/Ames Research Center

Dezfuli, Homayoon, NASA/HQ

Diehl, Roger, NASA/Jet Propulsion Laboratory

DiPietro, David, NASA/Goddard Space Flight Center

Doehne, Thomas, NASA/Glenn Research Center

Duarte, Alberto, NASA/Marshall Space Flight Center

Durham, David, NASA/Jet Propulsion Laboratory

Epps, Amy, NASA/Marshall Space Flight Center

Fashimpaur, Karen, Vantage Partners

Feikema, Douglas, NASA/Glenn Research Center

Fitts, David, NASA/Johnson Space Flight Center

Foster, Michele, NASA/Marshall Space Flight Center

Fuller, David, NASA/Glenn Research Center

Gati, Frank, NASA/Glenn Research Center

Gefert, Leon, NASA/Glenn Research Center

Ghassemieh, Shakib, NASA/Ames Research Center

Grantier, Julie, NASA/Glenn Research Center

Hack, Kurt, NASA/Glenn Research Center

Hall, Kelly, NASA/Glenn Research Center

Hamaker, Franci, NASA/Kennedy Space Center

Hange, Craig, NASA/Ames Research Center

Henry, Thad, NASA/Marshall Space Flight Center

Hill, Nancy, NASA/Marshall Space Flight Center

Hirshorn, Steven, NASA/Headquarters

Holladay, Jon, NASA/NASA Engineering and Safety Center

Hyatt, Mark, NASA/Glenn Research Center

Killebrew, Jana, NASA/Ames Research Center

Jannette, Tony, NASA/Glenn Research Center

Jenks, Kenneth, NASA/Johnson Space Center

Jones, Melissa, NASA/Jet Propulsion Laboratory

Jones, Ross, NASA/Jet Propulsion Laboratory

Killebrew, Jana, NASA/Ames Research Center

Leitner, Jesse, NASA/Goddard Space Flight Center

Lin, Chi, NASA/Jet Propulsion Laboratory

Mascia, Anne Marie, Graphic Artist

McKay, Terri, NASA/Marshall Space Flight Center

McNelis, Nancy, NASA/Glenn Research Center

Mendoza, Donald, NASA/Ames Research Center

Miller, Scott, NASA/Ames Research Center

Montgomery, Patty, NASA/Marshall Space Flight Center

Mosier, Gary, NASA/Goddard Space Flight Center

Noble, Lee, NASA/Langley Research Center

Oleson, Steven, NASA/Glenn Research Center

Parrott, Edith, NASA/Glenn Research Center

Powell, Christine, NASA/Stennis Space Center

Powell, Joseph, NASA/Glenn Research Center

Price, James, NASA/Langley Research Center

Rawlin, Adam, NASA/Johnson Space Center

Rochlis-Zumbado, Jennifer, NASA/Johnson Space Center

Rohn, Dennis, NASA/Glenn Research Center

Rosenbaum, Nancy, NASA/Goddard Space Flight Center

ix NASA SYSTEMS ENGINEERING HANDBOOK

Acknowledgments

Ryan, Victoria, NASA/Jet Propulsion Laboratory

Sadler, Gerald, NASA/Glenn Research Center

Salazar, George, NASA/Johnson Space Center

Sanchez, Hugo, NASA/Ames Research Center

Schuyler, Joseph, NASA/Stennis Space Center

Sheehe, Charles, NASA/Glenn Research Center

Shepherd, Christena, NASA/Marshall Space Flight Center

Shull, Thomas, NASA/Langley Research Center

Singer, Bart, NASA/Langley Research Center

Slywczak, Richard, NASA/Glenn Research Center

Smith, Scott, NASA/Goddard Space Flight Center

Smith, Joseph, NASA/Headquarters

Sprague, George, NASA/Jet Propulsion Laboratory

Trase, Kathryn, NASA/Glenn Research Center

Trenkle, Timothy, NASA/Goddard Space Flight Center

Vipavetz, Kevin, NASA/Langley Research Center

Voss, Linda, Dell Services

Walters, James Britton, NASA/Johnson Space Center

Watson, Michael, NASA/Marshall Space Flight Center

Weiland, Karen, NASA/Glenn Research Center

Wiedeman, Grace, Dell Services

Wiedenmannott, Ulrich, NASA/Glenn Research Center

Witt, Elton, NASA/Johnson Space Center

Woytach, Jeffrey, NASA/Glenn Research Center

Wright, Michael, NASA/Marshall Space Flight Center

Yu, Henry, NASA/Kennedy Space Center

x NASA SYSTEMS ENGINEERING HANDBOOK

1.0 Introduction

1.1 Purpose This handbook is intended to provide general guidance and information on systems engineer- ing that will be useful to the NASA community. It provides a generic description of Systems Engineering (SE) as it should be applied throughout NASA. A goal of the handbook is to increase awareness and consis- tency across the Agency and advance the practice of SE. This handbook provides perspectives relevant to NASA and data particular to NASA.

This handbook should be used as a companion for implementing NPR 7123.1, Systems Engineering Processes and Requirements, as well as the Center- specific handbooks and directives developed for implementing systems engineering at NASA. It pro- vides a companion reference book for the various systems engineering-related training being offered under NASA’s auspices.

1.2 Scope and Depth This handbook describes systems engineering best practices that should be incorporated in the develop- ment and implementation of large and small NASA programs and projects. The engineering of NASA

systems requires a systematic and disciplined set of processes that are applied recursively and iteratively for the design, development, operation, maintenance, and closeout of systems throughout the life cycle of the programs and projects. The scope of this hand- book includes systems engineering functions regard- less of whether they are performed by a manager or an engineer, in-house or by a contractor.

There are many Center-specific handbooks and direc- tives as well as textbooks that can be consulted for in-depth tutorials. For guidance on systems engi- neering for information technology projects, refer to Office of Chief Information Officer *Information Technology Systems Engineering Handbook Version 2.0*. For guidance on entrance and exit criteria for mile- stone reviews of software projects, refer to *NASA- HDBK-2203, NASA Software Engineering Handbook*. A NASA systems engineer can also participate in the NASA Engineering Network (NEN) Systems Engineering Community of Practice, located at *https://nen.nasa.gov/web/se*. This Web site includes many resources useful to systems engineers, includ- ing document templates for many of the work prod- ucts and milestone review presentations required by the NASA SE process.

1 NASA SYSTEMS ENGINEERING HANDBOOK

1.0 Introduction

This handbook is applicable to NASA space flight projects of all sizes and to research and development programs and projects. While all 17 processes are applicable to all projects, the amount of formality, depth of documentation, and timescales are varied as appropriate for the type, size, and complexity of the project. References to “documents” are intended to include not only paper or digital files but also models,

NASA SYSTEMS ENGINEERING HANDBOOK

graphics, drawings, or other appropriate forms that capture the intended information.

For a more in-depth discussion of the principles pro- vided in this handbook, refer to the NASA Expanded Guidance for SE document which can be found at *https://nen.nasa.gov/web/se/doc-repository*. This hand- book is an abridged version of that reference.

2

2.0 Fundamentals of Systems Engineering

At methodical, NASA, “systems engineering” is defined as a multi-disciplinary approach for the design, realization, technical management, opera- tions, and retirement of a system. A “system” is the combination of elements that function together to produce the capability required to meet a need. The elements include all hardware, software, equip- ment, facilities, personnel, processes, and procedures needed for this purpose; that is, all things required to produce system-level results. The results include sys- tem-level qualities, properties, characteristics, func- tions, behavior, and performance. The value added by the system as a whole, beyond that contributed inde- pendently by the parts, is primarily created by the relationship among the parts; that is, how they are interconnected.1 It is a way of looking at the “big pic- ture” when making technical decisions. It is a way of achieving stakeholder functional, physical, and oper- ational performance requirements in the intended use environment over the planned life of the system within cost, schedule, and other constraints. It is a methodology that supports the containment of the life cycle cost of a system. In other words, systems engineering is a logical way of thinking.

1 Eberhardt Rechtin, *Systems Architecting of Organizations:*

*Why Eagles Can’t Swim.*

Systems engineering is the art and science of devel- oping an operable system capable of meeting require- ments within often opposed constraints. Systems engineering is a holistic, integrative discipline, wherein the contributions of structural engineers, electrical engineers, mechanism designers, power engineers, human factors engineers, and many more disciplines are evaluated and balanced, one against another, to produce a coherent whole that is not dom- inated by the perspective of a single discipline.2

Systems engineering seeks a safe and balanced design in the face of opposing interests and multiple, some- times conflicting constraints. The systems engineer should develop the skill for identifying and focusing efforts on assessments to optimize the overall design and not favor one system/subsystem at the expense of another while constantly validating that the goals of the operational system will be met. The art is in knowing when and where to probe. Personnel with these skills are usually tagged as “systems engineers.” They may have other titles—lead systems engineer,

2 Comments on systems engineering throughout Chapter 2 .0 are extracted from the speech “System Engineering and the Two Cultures of Engineering” by Michael D . Griffin, NASA Administrator .

3 NASA SYSTEMS ENGINEERING HANDBOOK

2.0 Fundamentals of Systems Engineering

technical manager, chief engineer—but for this doc- ument, the term “systems engineer” is used.

The exact role and responsibility of the systems engi- neer may change from project to project depending on the size and complexity of the project and from phase to phase of the life cycle. For large projects, there may be one or more systems engineers. For small projects, the project manager may sometimes perform these practices. But whoever assumes those responsibil- ities, the systems engineering functions should be performed. The actual assignment of the roles and responsibilities of the named systems engineer may also therefore vary. The lead systems engineer ensures that the system technically fulfills the defined needs and requirements and that a proper systems engineer- ing approach is being followed. The systems engineer oversees the project’s systems engineering activities as performed by the technical team and directs, com- municates, monitors, and coordinates tasks. The systems engineer reviews and evaluates the technical aspects of the project to ensure that the systems/sub- systems engineering processes are functioning prop- erly and evolves the system from concept to product. The entire technical team is involved in the systems engineering process.

The systems engineer usually plays the key role in leading the development of the concept of opera- tions (ConOps) and resulting system architec- ture, defining boundaries, defining and allocating requirements, evaluating design tradeoffs, balanc- ing technical risk between systems, defining and assessing interfaces, and providing oversight of ver- ification and validation activities, as well as many other tasks. The systems engineer typically leads the technical planning effort and has the prime respon- sibility in documenting many of the technical plans, requirements and specification documents, verifica- tion and validation documents, certification pack- ages, and other technical documentation.

NASA SYSTEMS ENGINEERING HANDBOOK

In summary, the systems engineer is skilled in the art and science of balancing organizational, cost, and technical interactions in complex systems. The systems engineer and supporting organization are vital to supporting program and Project Planning and Control (PP&C) with accurate and timely cost and schedule information for the technical activities. Systems engineering is about tradeoffs and compro- mises; it uses a broad crosscutting view of the system rather than a single discipline view. Systems engineer- ing is about looking at the “big picture” and not only ensuring that they get the design right (meet require- ments) but that they also get the right design (enable operational goals and meet stakeholder expectations).

Systems engineering plays a key role in the project organization. Managing a project consists of three main objectives: managing the technical aspects of the project, managing the project team, and manag- ing the cost and schedule. As shown in FIGURE 2.0-1, these three functions are interrelated. Systems engi- neering is focused on the technical characteristics of decisions including technical, cost, and schedule and on providing these to the project manager. The Project Planning and Control (PP&C) function is responsible for identifying and controlling the cost and schedules of the project. The project manager has overall responsibility for managing the project team and ensuring that the project delivers a technically correct system within cost and schedule. Note that there are areas where the two cornerstones of project management, SE and PP&C, overlap. In these areas, SE provides the technical aspects or inputs whereas PP&C provides the programmatic, cost, and sched- ule inputs.

This document focuses on the SE side of the dia- gram. The practices/processes are taken from NPR 7123.1, NASA Systems Engineering Processes and Requirements. Each process is described in much greater detail in subsequent chapters of this

4

2.0 Fundamentals of Systems Engineering

PROJECT MANAGEMENT

PROJECT MANAGEMENT ACTIVITIES

• Setting up Project Team

• Identifying Programmatic Risks

• Programmatic Stakeholders (non-technical, non-business)

• Programmatic Planning (non-technical, non-business)

• Identifying Programmatic (non-technical) requirements

NASA SYSTEMS ENGINEERING HANDBOOK

• Technology Transfer and Commercialization

• Integration of technical and non-technical activities

• Overall Approver/Decider

Systems Engineering

System Design Processes

5

• Stakeholder Expectations Definition

• Technical Requirement’s Definition

• Logical Decomposition

• Design Solution Definition Product Realization Processes

• Product Implementation

• Product Integration

• Product Verification

• Product Validation

• Product Transition Technical Management Processes

• Technical Planning

• Requirements Management

• Interface Management

• Technical Risk Management

• Configuration Management

• Technical Data Management

• Technical Assessment

• Decision Analyses

Common Areas

• Stakeholders

• Risks

• Configuration Management

• Data Management

• Reviews

• Schedule

PP&C

PP&C

PP&C

• PP&C Integration

• PP&C Integration

• Resource Management

• Resource Management

• Scheduling

• Scheduling

• Scheduling

• Cost Estimation & Assessment

• Cost Estimation & Assessment

• Cost Estimation & Assessment

• Cost Estimation & Assessment

• Acquisition & Contract Management

• Acquisition & Contract Management

• Acquisition & Contract Management

• Acquisition & Contract Management

• Acquisition & Contract Management

• Risk Management

• Risk Management

• Risk Management

• CM/DM

• CM/DM

FIGURE 2.0-1 SE in Context of Overall Project Management

document, but an overview is given in the following subsections of this chapter.

2.1 The Common Technical Processes and the SE Engine

There are three sets of common technical processes in NPR 7123.1, NASA Systems Engineering Processes and Requirements: system design, product realiza- tion, and technical management. The processes in each set and their interactions and flows are illustrated

by the NPR systems engineering “engine” shown in FIGURE 2.1-1. The processes of the SE engine are used to develop and realize the end products. This chap- ter provides the application context of the 17 com- mon technical processes required in NPR7123.1. The system design processes, the product realization processes, and the technical management processes are discussed in more detail in *Chapters 4.0*, *5.0*, and *6.0*, respectively. Processes 1 through 9 indicated in FIGURE 2.1-1 represent the tasks in the execution of a project. Processes 10 through17 are crosscutting tools for carrying out the processes.

2.0 Fundamentals of Systems Engineering

**Requirements Flow Down from Level above**

**Technical Management Processes System Design Processes**

10. Technical Planning

11. Requirement Management 12. Interface Management 13. Technical Risk Management 14. Configuration Management 15. Technical Data Management

16. Technical Assessment

**Technical Decision Analysis Process**

17. Decision Analysis

NASA SYSTEMS ENGINEERING HANDBOOK

**Product Technical Planning**

**Processes**

**Realization Processes**

**Requirements Definition**

**Product Processes**

**Technical Control Processes**

System Design Processes applied to each product layer down through system structure

**Transition Processes**

1. Stakeholders Expectations

Definition 2. Technical Requirements

**Evaluation Processes** Definition

**Design Realization Technical Assessment Processes** 3. Logical Decomposition

**Processes** 4. Design Solution Definition

FIGURE 2.1-1 The Systems Engineering Engine (NPR 7123 .1)

• System Design Processes: The four system design processes shown in FIGURE 2.1-1 are used to define and baseline stakeholder expectations, gen- erate and baseline technical requirements, decom- pose the requirements into logical and behavioral models, and convert the technical requirements into a design solution that will satisfy the base- lined stakeholder expectations. These processes are applied to each product of the system struc- ture from the top of the structure to the bottom until the lowest products in any system structure branch are defined to the point where they can be built, bought, or reused. All other products in the

**Realized Products to Level above**

9. Product Transition Cross-

Cross- cutting

cutting

8. Product Validation 7. Product Verification

**Technical Solution Definition Processes**

6. Product Integration 5. Product Implementation

**Requirements Flow Down**

**Realized Products To Level below**

**From Level below**

Product Realization Processes applied to each product layer up through system structure

system structure are realized by implementation or integration.

• Product Realization Processes: The product real- ization processes are applied to each operational/ mission product in the system structure starting from the lowest level product and working up to higher level integrated products. These processes are used to create the design solution for each product (through buying, coding, building, or reusing) and to verify, validate, and transition up to the next hierarchical level those products that satisfy their design solutions and meet stakeholder

6

2.0 Fundamentals of Systems Engineering

expectations as a function of the applicable life cycle phase.

• Technical Management Processes: The techni- cal management processes are used to establish and evolve technical plans for the project, to man- age communication across interfaces, to assess progress against the plans and requirements for the system products or services, to control tech- nical execution of the project through to comple- tion, and to aid in the decision-making process.

TABLE 2.1-1 Alignment of the 17 SE Processes to AS9100

SE Process AS9100 Requirement

Stakeholder Expectations Customer Requirements

Technical Requirements Definition

NASA SYSTEMS ENGINEERING HANDBOOK

product or set of products to correct a discovered discrepancy or other variation from requirements,” whereas “recursive” is defined as adding value to the system “by the repeated application of processes to design next lower layer system products or to real- ize next upper layer end products within the system structure. This also applies to repeating application of the same processes to the system structure in the next life cycle phase to mature the system definition and satisfy phase success criteria.” The technical processes are applied recursively and iteratively to break down the initializing concepts of the system to a level of The processes within the SE engine are used both

detail concrete enough that the technical team can iteratively and recursively. As defined in NPR 7123.1,

implement a product from the information. Then “iterative” is the “application of a process to the same

the processes are applied recursively and iteratively to

Planning of Product Realization

Logical Decomposition Design and Development Input

Design Solution Definition Design and Development Output

Product Implementation Control of Production

Product Integration Control of Production

Product Verification Verification

Product Validation Validation

Product Transition Control of Work Transfers; Post Delivery Support, Preservation of Product

Technical Planning Planning of Product Realization; Review of Requirements; Measurement, Analysis and

Improvement

Requirements Management Design and Development Planning; Purchasing

Interface Management Configuration Management

Technical Risk Management Risk Management

Configuration Management Configuration Management; Identification and Traceability; Control of Nonconforming

Product

Technical Data Management Control of Documents; Control of Records; Control of Design and Development

Changes

Technical Assessment Design and Development Review

Decision Analysis Measurement, Analysis and Improvement; Analysis of Data

7

2.0 Fundamentals of Systems Engineering

integrate the smallest product into greater and larger 2.2 systems until the whole of the system or product has

NASA SYSTEMS ENGINEERING HANDBOOK

An Overview of the SE Engine by Project Phase been assembled, verified, validated, and transitioned.

FIGURE 2.2-1 conceptually illustrates how the SE engine is used during each phase of a project (Pre- For a detailed example of how the SE Engine could

Phase A through Phase F). The life cycle phases are be used, refer to the NASA Expanded Guidance

described in TABLE 2.2-1. FIGURE 2.2-1 is a *conceptual* for SE document at *https://nen.nasa.gov/web/se/*

diagram. For full details, refer to the poster version *doc-repository*.

of this figure, which is located at *https://nen.nasa.gov/ web/se/doc-repository*. AS9100 is a widely adopted and standardized qual- ity management system developed for the commer- cial aerospace industry. Some NASA Centers have chosen to certify to the AS9100 quality system and may require their contractors to follow NPR 7123.1. TABLE 2.1-1 shows how the 17 NASA SE processes align with AS9100.

Pre-Phase A: Concept Studies

The uppermost horizontal portion of this chart is used as a reference to project system maturity, as the project progresses from a feasible concept to an as-de- ployed system; phase activities; Key Decision Points (KDPs); and major project reviews. The next major horizontal band shows the technical development

Formulation

Approval

Implementation Phase C: Final Design & Fabrication

tnempoleveDl acinhceTt nemeganaMl acinhceTPhase A:

Phase B:

Phase D:

Phase E: Concept & Technology

Preliminary Design &

System Assembly,

Operations & Development

Technology Completion

Integration & Test, Launch

Sustainment

6.2

6.7

FIGURE 2.2-1 Miniature Version of the Poster-Size NASA Project Life Cycle Process Flow for Flight and Ground Systems Accompanying this Handbook

Phase F: Closeout

Feasible Concept Top-Level Architecture Functional Baseline Allocated Baseline Baseline

Product As-Deployed Baseline

Key Decision Points:

Major Reviews:

4.1

?

?

?

4.1 ?4.2

4.3

4.3

5.4

4.4 4.45.3?5.1

?

?

?

6.1

6.8 ?5.5

4.2

?

5.2

5.5

5.4

5.3

5.1

5.2

6.1

6.1

6.1

6.1

6.1

6.1

6.3

6.4

6.5

6.6

6.8

6.8

6.8

6.8

6.8

6.8

8

2.0 Fundamentals of Systems Engineering

TABLE 2.2-1 Project Life Cycle Phases

Phase Purpose Typical Outcomes

n oitalumroF-erPPre-Phase A

To produce a broad spectrum of ideas and alternatives

Feasible system concepts Concept

for missions from which new programs/projects can be

in the form of simulations, Studies

selected. Determine feasibility of desired system, develop

analysis, study reports, mission concepts, draft system-level requirements, assess

models, and mock-ups performance, cost, and schedule feasibility; identify potential technology needs, and scope.

Phase A

System concept definition Concept and

in the form of simulations, Technology

analysis, engineering models Development

and mock-ups, and trade study definition

Phase B Preliminary Design and Technology Completion

NASA SYSTEMS ENGINEERING HANDBOOK

To determine the feasibility and desirability of a suggested new system and establish an initial baseline compatibility with NASA’s strategic plans. Develop final mission concept, system-level requirements, needed system technology developments, and program/project technical management plans.

End products in the form of mock-ups, trade study results, specification and interface documents, and prototypes

Phase C Final Design and Fabrication

To define the project in enough detail to establish an initial baseline capable of meeting mission needs. Develop system structure end product (and enabling product) requirements and generate a preliminary design for each system structure end product.

End product detailed designs, end product component fabrication, and software development

Phase D System Assembly, Integration and Test, Launch

To complete the detailed design of the system (and its associated subsystems, including its operations systems), fabricate hardware, and code software. Generate final designs for each system structure end product.

Operations-ready system end product with supporting related enabling products

Phase E Operations and Sustainment

To assemble and integrate the system (hardware, software, and humans), meanwhile developing confidence that it is able to meet the system requirements. Launch and prepare for operations. Perform system end product implementation, assembly, integration and test, and transition to use.

Desired system

Phase F Closeout

To conduct the mission and meet the initially identified need and maintain support for that need. Implement the mission operations plan.

To implement the systems decommissioning/disposal plan

Product closeout developed in Phase E and perform analyses of the returned data and any returned samples.

processes (steps 1 through 9) in each project phase.

and closes out (Phase F), the technical work shifts The SE engine cycles five times from Pre-Phase A

to activities commensurate with these last two proj- through Phase D. Note that NASA’s management

ect phases. The next major horizontal band shows has structured Phases C and D to “split” the tech-

the eight technical management processes (steps 10 nical development processes in half in Phases C and

through 17) in each project phase. The SE engine D to ensure closer management control. The engine

cycles the technical management processes seven is bound by a dashed line in Phases C and D. Once

times from Pre-Phase A through Phase F. a project enters into its operational state (Phase E)

9

2.0 Fundamentals of Systems Engineering

2.3 Example of Using the SE Engine In Pre-Phase A, the SE engine is used to develop the initial concepts; clearly define the unique roles of humans, hardware, and software in performing the missions objectives; establish the system functional and performance boundaries; develop/identify a pre- liminary/draft set of key high-level requirements, define one or more initial Concept of Operations (ConOps) scenarios; realize these concepts through iterative modeling, mock-ups, simulation, or other means; and verify and validate that these concepts and products would be able to meet the key high-level requirements and ConOps. The operational concept must include scenarios for all significant operational situations, including known off-nominal situations. To develop a useful and complete set of scenarios, important malfunctions and degraded-mode opera- tional situations must be considered. The importance of early ConOps development cannot be underesti- mated. As system requirements become more detailed and contain more complex technical information, it becomes harder for the stakeholders and users to understand what the requirements are conveying; i.e., it may become more difficult to visualize the end product. The ConOps can serve as a check in identi- fying missing or conflicting requirements.

Note that this Pre-Phase A initial concepts develop- ment work is not the formal verification and valida- tion program that is performed on the final product, but rather it is a methodical run through ensuring that the concepts that are being developed in this Pre-Phase A are able to meet the likely requirements and expectations of the stakeholders. Concepts are developed to the lowest level necessary to ensure that they are feasible and to a level that reduces the risk low enough to satisfy the project. Academically, this process could proceed down to the circuit board level for every system; however, that would involve a great deal of time and money. There may be a higher level or tier of product than circuit board level that would

NASA SYSTEMS ENGINEERING HANDBOOK

enable designers to accurately determine the feasibil- ity of accomplishing the project, which is the purpose of Pre-Phase A.

During Phase A, the recursive use of the SE engine is continued, this time taking the concepts and draft key requirements that were developed and validated during Pre-Phase A and fleshing them out to become the set of baseline system requirements and ConOps. During this phase, key areas of high risk might be simulated to ensure that the concepts and require- ments being developed are good ones and to identify verification and validation tools and techniques that will be needed in later phases.

During Phase B, the SE engine is applied recursively to further mature requirements and designs for all products in the developing product tree and perform verification and validation of concepts to ensure that the designs are able to meet their requirements. Operational designs and mission scenarios are evalu- ated and feasibility of execution within design capa- bilities and cost estimates are assessed.

Phase C again uses the left side of the SE engine to finalize all requirement updates, finalize the ConOps validation, develop the final designs to the lowest level of the product tree, and begin fabrication.

Phase D uses the right side of the SE engine to recur- sively perform the final implementation, integration, verification, and validation of the end product, and at the final pass, transition the end product to the user.

The technical management processes of the SE engine are used in Phases E and F to monitor performance; control configuration; and make decisions associ- ated with the operations, sustaining engineering, and closeout of the system. Any new capabilities or upgrades of the existing system reenter the SE engine as new developments.

10

2.0 Fundamentals of Systems Engineering

2.4 Distinctions between Product Verification and Product Validation

From a process perspective, the Product Verification and Product Validation processes may be similar in nature, but the objectives are fundamentally different:

• Verification of a product shows proof of compli- ance with requirements—that the product can meet each “shall” statement as proven though per- formance of a test, analysis, inspection, or demon- stration (or combination of these).

• Validation of a product shows that the prod- uct accomplishes the intended purpose in the intended environment—that it meets the expec- tations of the customer and other stakeholders as shown through performance of a test, analysis, inspection, or demonstration.

Verification testing relates back to the approved requirements set and can be performed at different stages in the product life cycle. The approved specifi- cations, drawings, parts lists, and other configuration documentation establish the configuration baseline of that product, which may have to be modified at a later time. Without a verified baseline and appropri- ate configuration controls, later modifications could be costly or cause major performance problems.

Validation relates back to the ConOps document. Validation testing is conducted under realistic con- ditions (or simulated conditions) on end products for the purpose of determining the effectiveness and suit- ability of the product for use in mission operations by typical users. Validation can be performed in each development phase using phase products (e.g., mod- els) and not only at delivery using end products.

NASA SYSTEMS ENGINEERING HANDBOOK

It is appropriate for verification and validation meth- ods to differ between phases as designs advance. The ultimate success of a program or project may relate to the frequency and diligence of validation efforts during the design process, especially in Pre-Phase A and Phase A during which corrections in the direc- tion of product design might still be made cost-effec- tively. The question should be continually asked, “Are we building the right product for our users and other stakeholders?” The selection of the verification or val- idation method is based on engineering judgment as to which is the most effective way to reliably show the product’s conformance to requirements or that it will operate as intended and described in the ConOps.

2.5 Cost Effectiveness Considerations

The objective of systems engineering is to see that the system is designed, built, and can be operated so that it accomplishes its purpose safely in the most cost-ef- fective way possible considering performance, cost, schedule, and risk. A cost-effective and safe system should provide a particular kind of balance between effectiveness and cost. This causality is an indefinite one because there are usually many designs that meet the cost-effective condition.

Design trade studies, an important part of the sys- tems engineering process, often attempt to find designs that provide the best combination of cost and effectiveness. At times there are alternatives that either reduce costs without reducing effectiveness or increase effectiveness without increasing cost. In such “win-win” cases, the systems engineer’s decision is easy. When the alternatives in a design trade study require trading cost for effectiveness, the decisions become harder.

11

2.0 Fundamentals of Systems Engineering

THE SYSTEMS ENGINEER’S DILEMMA

At each cost-effective solution:

• To reduce cost at constant risk, performance must be reduced.

• To reduce risk at constant cost, performance must be reduced.

• To reduce cost at constant performance, higher risks must be accepted.

• To reduce risk at constant performance, higher costs must be accepted.

In this context, time in the schedule is often a critical resource, so that *schedule* behaves like a kind of *cost*.

FIGURE 2.5-1 shows that the life cycle costs of a

The technical team may have to choose among designs program or project tend to get “locked in” early in

that differ in terms of numerous attributes. A variety of design and development. The cost curves clearly show

methods have been developed that can be used to help that late identification of and fixes to problems cost

uncover preferences between attributes and to quan- considerably more later in the life cycle. Conversely,

tify subjective assessments of relative value. When descopes taken later versus earlier in the project life

this can be done, trades between attributes can be cycle result in reduced cost savings. This figure,

assessed quantitatively. Often, however, the attributes obtained from the Defense Acquisition University, is

are incompatible. In the end, decisions need to be an example of how these costs are determined by the

made in spite of the given variety of attributes. There early concepts and designs. The numbers will vary

are several decision analysis techniques (*Section 6.8*) from project to project, but the general shape of the

that can aid in complex decision analysis. The systems curves and the message they send will be similar. For

engineer should always keep in mind the information example, the figure shows that during design, only

that needs to be available to help the decision-makers about 15% of the costs might be expended, but the

choose the most cost-effective option. design itself will commit about 75% of the life cycle costs. This is because the way the system is designed will determine how expensive it will be to test, man- 2.6 Human Systems Integration ufacture, integrate, operate, and sustain. If these fac-

(HSI) in the SE Process tors have not been considered during design, they pose significant cost risks later in the life cycle. Also

As noted at the beginning of NPR 7123.1, the “sys- note that the cost to change the design increases as

tems approach is applied to all elements of a system you get later in the life cycle. If the project waits until

(i.e., hardware, software, human systems integra- verification to do any type of test or analysis, any

tion. In short, the systems engineering approach problems found will have a significant cost impact to

must equally address and integrate these three key redesign and reverify.

elements: hardware, software, and human systems

NASA SYSTEMS ENGINEERING HANDBOOK

12

2.0 Fundamentals of Systems Engineering

e miTt sniagat soCe lcyCe fiLe gatnecrePe vitalumuC100%

NASA SYSTEMS ENGINEERING HANDBOOK

90% 90%

80%

70%

50%

Co75% mCmycCitle otesCd t 20–100× oto LsitfCs e hange (% CDoeCssoigts mn 500–1000× EpDxleirpeteecnd tdioen d)

50%

100%

20% 8% 15% Time

MCR Mission Concept Review CDR Critical Design Review

SRR System Requirements Review SIR System Integration Review

SDR System Definition Review ORR Operational Readiness Review

PDR Preliminary Design Review DR/DRR Decommissioning/Disposal Readiness Review

Adapted from INCOSE-TP-2003-002-04, 2015

FIGURE 2.5-1 Life-Cycle Cost Impacts from Early Phase Decision-Making

2.7 Competency Model for Systems Engineers

TABLE 2.7-1 provides a summary of the Competency Model for Systems Engineering. For more informa- tion on the NASA SE Competency model refer to: *http://appel.nasa.gov/competency-model/*.

There are four levels of proficiencies associated with each of these competencies:

• Team Practitioner/Technical Engineer

• Team Lead/Subsystem Lead

• Project Systems Engineer

• Chief Engineer Operations through 60%

Disposal

45%

40% 3–6×

30%

Concept Design

Develop

Prod/Test

20%

10%

0%

MCR SRR SDR PDR CDR SIR ORR DR/DRR

integration. Therefore, the human element is some- thing that integration and systems engineering pro- cesses must address. The definition of “system” in NPR 7123.1 is inclusive; i.e., a system is “the combi- nation of elements that function together to produce the capability required to meet a need. The elements include all hardware, software, equipment, facilities, personnel, processes, and procedures needed for this purpose. For additional information and guidance on his, refer to Section 2.6 of the NASA Expanded Guidance for Systems Engineering at *https://nen. nasa.gov/web/se/doc-repository*.

13

2.0 Fundamentals of Systems Engineering

TABLE 2.7-1 NASA System Engineering Competency Model

Competency

Competency Description Area

SE 1.0 System Design

NASA SYSTEMS ENGINEERING HANDBOOK

SE 1.1 Stakeholder Expectation Definition & Management

Eliciting and defining use cases, scenarios, concept of operations and stakeholder expectations. This includes identifying stakeholders, establishing support strategies, establishing a set of Measures of Effectiveness (MOEs), validating stakeholder expectation statements, and obtaining commitments from the customer and other stakeholders, as well as using the baselined stakeholder expectations for product validation during product realization

SE 1.2 Technical Requirements Definition

Transforming the baseline stakeholder expectations into unique, quantitative, and measurable technical requirements expressed as “shall” statements that can be used for defining the design solution. This includes analyzing the scope of the technical problems to be solved, defining constraints affecting the designs, defining the performance requirements, validating the resulting technical requirement statements, defining the Measures of Performance (MOPs) for each MOE, and defining appropriate Technical Performance Measures (TPMs) by which technical progress will be assessed.

SE 1.3 Logical Decomposition

Transforming the defined set of technical requirements into a set of logical decomposition models and their associated set of derived technical requirements for lower levels of the system, and for input to the design solution efforts. This includes decomposing and analyzing by function, time, behavior, data flow, object, and other models. It also includes allocating requirements to these decomposition models, resolving conflicts between derived requirements as revealed by the models, defining a system architecture for establishing the levels of allocation, and validating the derived technical requirements.

SE 1.4 Design Solution Definition

Translating the decomposition models and derived requirements into one or more design solutions, and using the Decision Analysis process to analyze each alternative and for selecting a preferred alternative that will satisfy the technical requirements. A full technical data package is developed describing the selected solution. This includes generating a full design description for the selected solution; developing a set of ‘make-to,’ ‘buy-to,’ ‘reuse-to,’ specifications; and initiating the development or acquisition of system products and enabling products.

SE 2.0 Product Realization

SE 2.1 Product Implementation

Generating a specific product through buying, making, or reusing so as to satisfy the design requirements. This includes preparing the implementation strategy; building or coding the produce; reviewing vendor technical information; inspecting delivered, built, or reused products; and preparing product support documentation for integration.

SE 2.2 Product Integration

Assembling and integrating lower-level validated end products into the desired end product of the higher-level product. This includes preparing the product integration strategy, performing detailed planning, obtaining products to integrate, confirming that the products are ready for integration, preparing the integration environment, and preparing product support documentation.

SE 2.3 Product Verification

Proving the end product conforms to its requirements. This includes preparing for the verification efforts, analyzing the outcomes of verification (including identifying anomalies and establishing recommended corrective actions), and preparing a product verification report providing the evidence of product conformance with the applicable requirements.

(continued)

14

2.0 Fundamentals of Systems Engineering

Competency

Competency Description Area

SE 2.0 Product Realization

NASA SYSTEMS ENGINEERING HANDBOOK

SE 2.4 Product Validation

Confirming that a verified end product satisfies the stakeholder expectations for its intended use when placed in its intended environment and ensuring that any anomalies discovered during validation are appropriately resolved prior to product transition. This includes preparing to conduct product validation, performing the product validation, analyzing the results of validation (including identifying anomalies and establishing recommended corrective actions), and preparing a product validation report providing the evidence of product conformance with the stakeholder expectations baseline.

SE 2.5 Product Transition

Transitioning the verified and validated product to the customer at the next level in the system structure. This includes preparing to conduct product transition, evaluating the product and enabling product readiness for product transition, preparing the product for transition (including handling, storing, and shipping preparation), preparing sites, and generating required documentation to accompany the product

SE 3.0 Technical Management

SE 3.1 Technical Planning

Planning for the application and management of each common technical process, as well as identifying, defining, and planning the technical effort necessary to meet project objectives. This includes preparing or updating a planning strategy for each of the technical processes, and determining deliverable work products from technical efforts; identifying technical reporting requirements; identifying entry and success criteria for technical reviews; identifying product and process measures to be used; identifying critical technical events; defining cross domain interoperability and collaboration needs; defining the data management approach; identifying the technical risks to be addressed in the planning effort; identifying tools and engineering methods to be employed; and defining the approach to acquire and maintain technical expertise needed. This also includes preparing the Systems Engineering Management Plan (SEMP) and other technical plans; obtaining stakeholder commitments to the technical plans; and issuing authorized technical work directives to implement the technical work

SE 3.2 Requirements Management

Managing the product requirements, including providing bidirectional traceability, and managing changes to establish requirement baselines over the life cycle of the system products. This includes preparing or updating a strategy for requirements management; selecting an appropriate requirements management tool; training technical team members in established requirement management procedures; conducting expectation and requirements traceability audits; managing expectation and requirement changes; and communicating expectation and requirement change information

SE 3.3 Interface Management

Establishing and using formal interface management to maintain internal and external interface definition and compliance among the end products and enabling products. This includes preparing interface management procedures, identifying interfaces, generating and maintaining interface documentation, managing changes to interfaces, disseminating interface information, and conducting interface control

SE 3.4 Technical Risk Management

Examining on a continual basis the risks of technical deviations from the plans, and identifying potential technical problems before they occur. Planning, invoking, and performing risk-handling activities as needed across the life of the product or project to mitigate impacts on meeting technical objectives. This includes developing the strategy for technical risk management, identifying technical risks, and conducting technical risk assessment; preparing for technical risk mitigation, monitoring the status of each technical risk, and implementing technical risk mitigation and contingency action plans when applicable thresholds have been triggered.

(continued)

15

2.0 Fundamentals of Systems Engineering

Competency

Competency Description Area

SE 3.0 Technical Management

NASA SYSTEMS ENGINEERING HANDBOOK

SE 3.5 Configuration Management

Identifying the configuration of the product at various points in time, systematically controlling changes to the configuration of the product, maintaining the integrity and traceability of product configuration, and preserving the records of the product configuration throughout its life cycle. This includes establishing configuration management strategies and policies, identifying baselines to be under configuration control, maintaining the status of configuration documentation, and conducting configuration audits

SE 3.6 Technical Data Management

Identifying and controlling product-related data throughout its life cycle; acquiring, accessing, and distributing data needed to develop, manage, operate, support, and retire system products; managing and disposing data as records; analyzing data use; obtaining technical data feedback for managing the contracted technical efforts; assessing the collection of appropriate technical data and information; maintaining the integrity and security of the technical data, effectively managing authoritative data that defines, describes, analyzes, and characterizes a product life cycle; and ensuring consistent, repeatable use of effective Product Data and Life-cycle Management processes, best practices, interoperability approaches, methodologies, and traceability. This includes establishing technical data management strategies and policies; maintaining revision, status, and history of stored technical data and associated metadata; providing approved, published technical data; providing technical data to authorized parties; and collecting and storing required technical data.

SE 3.7 Technical Assessment

Monitoring progress of the technical effort and providing status information for support of the system design, product realization, and technical management efforts. This includes developing technical assessment strategies and policies, assessing technical work productivity, assessing product quality, tracking and trending technical metrics, and conducting technical, peer, and life cycle reviews.

SE 3.8 Technical Decision Analysis

Evaluating technical decision issues, identifying decision criteria, identifying alternatives, analyzing alternatives, and selecting alternatives. Performed throughout the system life cycle to formulate candidate decision alternatives, and evaluate their impacts on health and safety, technical, cost, and schedule performance. This includes establishing guidelines for determining which technical issues are subject to formal analysis processes; defining the criteria for evaluating alternative solutions; identifying alternative solutions to address decision issues; selecting evaluation methods; selecting recommended solutions; and reporting the results and findings with recommendations, impacts, and corrective actions.

16

3.0 NASA Program/Project Life Cycle

One NASA of the for fundamental the management concepts of major used systems within

is the program/project life cycle, which categorizes everything that should be done to accomplish a pro- gram or project into distinct phases that are separated by Key Decision Points (KDPs). *KDPs are the events at which the decision authority determines the readi- ness of a program/project to progress to the next phase of the life cycle (or to the next KDP).* Phase boundaries are defined so that they provide natural points for “go” or “no-go” decisions. Decisions to proceed may be qualified by liens that should be removed within an agreed-to time period. A program or project that fails to pass a KDP may be allowed to try again later after addressing deficiencies that precluded passing the KDP, or it may be terminated.

All systems start with the recognition of a need or the discovery of an opportunity and proceed through var- ious stages of development to the end of the project. While the most dramatic impacts of the analysis and optimization activities associated with systems engineer- ing are obtained in the early stages, decisions that affect cost continue to be amenable to the systems approach even as the end of the system lifetime approaches.

Decomposing the program/project life cycle into phases organizes the entire process into more man- ageable pieces. The program/project life cycle should provide managers with incremental visibility into the progress being made at points in time that fit with the management and budgetary environments.

For NASA projects, the life cycle is defined in the applicable governing document:

• For space flight projects: NPR 7120.5, NASA Space Flight Program and Project Management Requirements

• For information technology: NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements

• For NASA research and technology: NPR 7120.8, NASA Research and Technology Program and Project Management Requirements

• For software: NPR 7150.2 NASA Software Engineering Requirements

17 NASA SYSTEMS ENGINEERING HANDBOOK

3.0 NASA Program/Project Life Cycle

For example, NPR 7120.5 defines the major NASA

• Phase D: System Assembly, Integration and Test, life cycle phases as Formulation and Implementation.

Launch For space flight systems projects, the NASA life cycle

• Phase E: Operations and Sustainment phases of Formulation and Implementation divide

• Phase F: Closeout into the following seven incremental pieces. The phases of the project life cycle are:

FIGURE 3.0-1 is taken from NPR 7120.5 and provides the life cycle for NASA space flight projects and identi- Program Pre-Formulation:

fies the KDPs and reviews that characterize the phases.

• Pre-Phase A: Concept Studies

More information concerning life cycles can be found in the NASA Expanded Guidance for SE document at Program Formulation

*https://nen.nasa.gov/web/se/doc-repository* and in the

• Phase A: Concept and Technology Development

*SP-2014-3705, NASA Space Flight Program and Project*

• Phase B: Preliminary Design and Technology

*Management Handbook*. Completion

TABLE 3.0-1 is taken from NPR 7123.1 and represents Program Implementation:

the product maturity for the major SE products

• Phase C: Final Design and Fabrication

developed and matured during the product life cycle.

NASA Life-Cycle Phases Approval Formulation for

FORMULATION Implementation

Approval for

IMPLEMENTATION

Project Life-Cycle

Pre-Phase A:

Phase A:

Phase B:

Phase C:

Phase D:

Phase E:

Phase F: Phases

Concept Studies

Concept and

Preliminary Design

Final Design and

System Assembly,

Operations and

Closeout Technology

and Technology

Fabrication

Integration & Test,

Sustainment Development

Completion

Launch & Checkout

Project Life-

KDP A Cycle Gates,

FAD

FA Documents, and Major Events

Preliminary Project Requirements

Preliminary Project Plan

Baseline Project Plan

Launch End of Mission Final Archival of Data

Agency Reviews

Human Space Flight Project Life-Cycle

MCR

Reviews1,2

Inspections and

Re-flights

Refurbishment

Robotic Mission Project Life Cycle Reviews1,2

MCR

Other Reviews

Supporting Reviews

FOOTNOTES

ACRONYMS

MDR – Mission Definition Review 1. Flexibility is allowed as to the timing, number, and content of reviews as long as the equivalent

ASM – Acquisition Strategy Meeting

MRR – Mission Readiness Review information is provided at each KDP and the approach is fully documented in the Project Plan.

CDR – Critical Design Review

ORR – Operational Readiness Review 2. Life-cycle review objectives and expected maturity states for these reviews and the attendant

CERR – Critical Events Readiness Review

PDR – Preliminary Design Review KDPs are contained in Table 2-5 and Appendix D Table D-3 of this handbook

DR – Decommissioning Review

PFAR – Post-Flight Assessment Review 3. PRR is needed only when there are multiple copies of systems. It does not require an SRB. Timing

DRR – Disposal Readiness Review

PLAR – Post-Launch Assessment Review is notional.

FA – Formulation Agreement

PRR – Production Readiness Review 4. CERRs are established at the discretion of program .

FAD – Formulation Authorization Document

SAR – System Acceptance Review 5. For robotic missions, the SRR and the MDR may be combined.

FRR – Flight Readiness Review

SDR – System Definition Review 6. SAR generally applies to human space flight.

KDP – Key Decision Point

SIR – System Integration Review 7. Timing of the ASM is determined by the MDAA. It may take place at any time during Phase A.

LRR – Launch Readiness Review

SMSR – Safety and Mission Success Review Red triangles represent life-cycle reviews that require SRBs. The Decision Authority,

LV – Launch Vehicle

SRB – Standing Review Board Administrator, MDAA, or Center Director may request the SRB to conduct other reviews.

MCR – Mission Concept Review

SRR – System Requirements Review

FIGURE 3.0-1 NASA Space Flight Project Life Cycle from NPR 7120 .5E

NASA SYSTEMS ENGINEERING HANDBOOK

ASM7SRR

SRR

Peer Reviews, Subsystem PDFs, Subsystem CDRs, and System Reviews

KDP B KDP C KDP D KDP F KDP E

PDR SDR

Re-enters appropriate life-cycle phase if modifications are needed between flights

MDR5

PDR

CDR/ PRR3

CDR/ PRR3

SIR

SIR

FRR ORR

ORR

MRR

PLAR

CERR4

PLAR

CERR4

SAR6

SMSR,LRR (LV), FRR (LV) DREnd of Flight PFARDR

DRR

DRR

18

3.0 NASA Program/Project Life Cycle

TABLE 3.0-1 SE Product Maturity from NPR 7123 .1

Formulation Implementation

Uncoupled/ Loosely Coupled KDP 0 KDP I Periodic KDPs s tcudorPTightly Programs Projects Single Project Coupled

and

KDP 0 KDP I KDP II KDP III Periodic KDPs

Programs

NASA SYSTEMS ENGINEERING HANDBOOK

Pre- Phase A Phase A Phase B Phase C Phase D Phase E Phase F

KDP A KDP B KDP C KDP D KDP E KDP F

MCR SRR MDR/SDR PDR CDR SIR ORR FRR DR DRR

Stakeholder identification and \*\*Baseline Update Update Update

Concept definition \*\*Baseline Update Update Update Update

Measure of effectiveness definition

\*\*Approve

Cost and schedule for technical Initial Update Update Update Update Update Update Update Update

SEMP1 Preliminary \*\*Baseline \*\*Baseline Update Update Update

Requirements Preliminary \*\*Baseline Update Update Update

Technical Performance Measures definition

\*\*Approve

Architecture definition \*\*Baseline

Allocation of requirements to next lower level

\*\*Baseline

Required leading indicator trends

\*\*Initial Update Update Update

Design solution definition Preliminary \*\*Preliminary \*\*Baseline Update Update

Interface definition(s) Preliminary Baseline Update Update

Implementation plans (Make/ code, buy, reuse)

Preliminary Baseline Update

Integration plans Preliminary Baseline Update \*\*Update

Verification and validation plans

Approach Preliminary Baseline Update Update

Verification and validation results

\*\*Initial \*\*Preliminary \*\*Baseline

Transportation criteria and instructions

Initial Final Update

Operations plans Baseline Update Update \*\*Update

Operational procedures Preliminary Baseline \*\*Update Update

Certification (flight/use) Preliminary \*\*Final

Decommissioning plans Preliminary Preliminary Preliminary \*\*Baseline Update \*\*Update

Disposal plans Preliminary Preliminary Preliminary \*\*Baseline Update Update \*\*Update

\*\* Item is a required product for that review

1 SEMP is baselined at SRR for projects, tightly coupled programs and single-project programs, and at MDR/SDR for uncoupled,

and loosely coupled programs .

19

3.0 NASA Program/Project Life Cycle

3.1 Program Formulation The program Formulation Phase establishes a cost-ef- fective program that is demonstrably capable of meeting Agency and mission directorate goals and objectives. The program Formulation Authorization Document (FAD) authorizes a Program Manager (PM) to initiate the planning of a new program and to perform the analyses required to formulate a sound program plan. The lead systems engineer provides the technical planning and concept development or this phase of the program life cycle. Planning includes identifying the major technical reviews that are needed and associated entrance and exit criteria. Major reviews leading to approval at KDP I are the SRR, SDR, PDR, and governing Program Management

NASA SYSTEMS ENGINEERING HANDBOOK

Council (PMC) review. A summary of the required gate products for the program Formulation Phase can be found in the governing NASA directive (e.g., NPR 7120.5 for space flight programs, NPR 7120.7 for IT projects, NPR 7120.8 for research and tech- nology projects). Formulation for all program types is the same, involving one or more program reviews followed by KDP I where a decision is made approv- ing a program to begin implementation.

3.2 Program Implementation During the program Implementation phase, the PM works with the Mission Directorate Associate Administrator (MDAA) and the constituent project

20

SPACE FLIGHT PROGRAM FORMULATION

Purpose To establish a cost-effective program that is demonstrably capable of meeting Agency and mission directorate goals and objectives

Typical Activities and Their Products for Space Flight Programs

• Identify program stakeholders and users

• Develop program requirements based on user expectations and allocate them to initial projects

• Identify NASA risk classification

• Define and approve program acquisition strategies

• Develop interfaces to other programs

• Start developing technologies that cut across multiple projects within the program

• Derive initial cost estimates and approve a program budget based on the project’s life cycle costs

• Perform required program Formulation technical activities defined in NPR 7120.5

• Satisfy program Formulation reviews’ entrance/success criteria detailed in NPR 7123.1

• Develop a clear vision of the program’s benefits and usage in the operational era and document it in a ConOps Reviews

• MCR (pre-Formulation)

• SRR

• SDR

3.0 NASA Program/Project Life Cycle

SPACE FLIGHT PROGRAM IMPLEMENTATION

Purpose To execute the program and constituent projects and ensure that the program continues to contribute to Agency goals and objectives within funding constraints

Typical Activities and Their Products

• Initiate projects through direct assignment or competitive process (e.g., Request for Proposal (RFP), Announcement of Opportunity (AO)

• Monitor project’s formulation, approval, implementation, integration, operation, and ultimate decommissioning

• Adjust program as resources and requirements change

• Perform required program Implementation technical activities from NPR 7120.5

• Satisfy program Implementation reviews’ entrance/success criteria from NPR 7123.1

Reviews

• PSR/PIR (uncoupled and loosely coupled programs only)

• Reviews synonymous (not duplicative) with the project reviews in the project life cycle (see FIGURE 3.0-4) through Phase D (single-project and tightly coupled programs only)

managers to execute the program plan cost-effec- 3.3 Project Pre-Phase A: tively. Program reviews ensure that the program continues to contribute to Agency and mission

Concept Studies

directorate goals and objectives within funding con-

The purpose of Pre-Phase A is to produce a broad straints. A summary of the required gate products for

spectrum of ideas and alternatives for missions the program Implementation Phase can be found in

from which new programs/projects can be selected. the governing NASA directive; e.g., NPR 7120.5 for

During Pre-Phase A, a study or proposal team anal- space flight programs. The program life cycle has two

yses a broad range of mission concepts that can fall different implementation paths, depending on pro-

within technical, cost, and schedule constraints and gram type. Each implementation path has different

that contribute to program and Mission Directorate types of major reviews. It is important for the sys-

goals and objectives. Pre-Phase A effort could include tems engineer to know what type of program a proj-

focused examinations on high-risk or high tech- ect falls under so that the appropriate scope of the

nology development areas. These advanced studies, technical work, documentation requirements, and set

along with interactions with customers and other of reviews can be determined.

potential stakeholders, help the team to identify promising mission concept(s). The key stakehold- ers (including the customer) are determined and

NASA SYSTEMS ENGINEERING HANDBOOK

21

3.0 NASA Program/Project Life Cycle

SPACE FLIGHT PRE‐PHASE A: CONCEPT STUDIES

Purpose To produce a broad spectrum of ideas and alternatives for missions from which new programs and projects can be selected. Determine feasibility of desired system; develop mission concepts; draft system-level requirements; assess performance, cost, and schedule feasibility; identify potential technology needs and scope.

Typical Activities and Products

• Review/identify any initial customer requirements or scope of work, which may include:

> Mission > Science > Top-level system

• Identify and involve users and other stakeholders

> Identify key stakeholders for each phase of the life cycle > Capture and baseline expectations as Needs, Goals, and Objectives (NGOs) > Define measures of effectiveness

• Develop and baseline the Concept of Operations

> Identify and perform trade-offs and analyses of alternatives (AoA) > Perform preliminary evaluations of possible missions

• Identify risk classification

• Identify initial technical risks

• Identify the roles and responsibilities in performing mission objectives (i.e., technical team, flight, and ground crew) including training

• Develop plans

> Develop preliminary SEMP > Develop and baseline Technology Development Plan > Define preliminary verification and validation approach

• Prepare program/project proposals, which may include:

> Mission justification and objectives; > A ConOps that exhibits clear understanding of how the program’s outcomes will cost-effectively

satisfy mission objectives; > High-level Work Breakdown Structures (WBSs); > Life cycle rough order of magnitude (ROM) cost, schedule, and risk estimates; and > Technology assessment and maturation strategies.

• Satisfy MCR entrance/success criteria from NPR 7123.1

Reviews

• MCR

• Informal proposal review

NASA SYSTEMS ENGINEERING HANDBOOK

22

3.0 NASA Program/Project Life Cycle

expectations for the project are gathered from them. If feasible concepts can be found, one or more may be selected to go into Phase A for further development. Typically, the system engineers are heavily involved in the development and assessment of the concept options. In projects governed by NPR 7120.5, the descope options define what the system can accom- plish if the resources are not available to accomplish the entire mission. This could be in the form of fewer instruments, a less ambitious mission profile, accom- plishing only a few goals, or using cheaper, less capa- ble technology. Descope options can also reflect what the mission can accomplish in case a hardware fail- ure results in the loss of a portion of the spacecraft architecture; for example, what an orbiter can accom- plish after the loss of a lander. The success criteria are reduced to correspond with a descoped mission.

Descope options are developed when the NGOs or other stakeholder expectation documentation is developed. The project team develops a preliminary set of mission descope options as a gate product for the MCR, but these preliminary descope options are not baselined or maintained. They are kept in the documentation archive in case they are needed later in the life cycle.

It is important in Pre-Phase A to define an accurate group of stakeholders and users to help ensure that mission goals and operations concepts meet the needs and expectations of the end users. In addition, it is important to estimate the composition of the techni- cal team and identify any unique facility or personnel requirements.

Advanced studies may extend for several years and are typically focused on establishing mission goals and formulating top-level system requirements and ConOps. Conceptual designs may be developed to demonstrate feasibility and support programmatic estimates. The emphasis is on establishing feasibility

NASA SYSTEMS ENGINEERING HANDBOOK

and desirability rather than optimality. Analyses and designs are accordingly limited in both depth and number of options, but each option should be eval- uated for its implications through the full life cycle, i.e., through Operations and Disposal. It is important in Pre-Phase A to develop and mature a clear vision of what problems the proposed program will address, how it will address them, and how the solution will be feasible and cost-effective.

3.4 Project Phase A: Concept and Technology Development

The purpose of Phase A is to develop a proposed mission/system architecture that is credible and responsive to program expectations, requirements, and constraints on the project, including resources. During Phase A, activities are performed to fully develop a baseline mission concept, begin or assume responsibility for the development of needed tech- nologies, and clarify expected reliance on human elements to achieve full system functionality or autonomous system development. This work, along with interactions with stakeholders, helps mature the mission concept and the program requirements on the project. Systems engineers are heavily involved during this phase in the development and assessment of the architecture and the allocation of requirements to the architecture elements.

In Phase A, a team—often associated with a program or informal project office—readdresses the mission concept first developed in Pre-Phase A to ensure that the project justification and practicality are sufficient to warrant a place in NASA’s budget. The team’s effort focuses on analyzing mission requirements and estab- lishing a mission architecture. Activities become for- mal, and the emphasis shifts toward optimizing the concept design. The effort addresses more depth and considers many alternatives. Goals and objectives are

23

3.0 NASA Program/Project Life Cycle

SPACE FLIGHT PHASE A: CONCEPT AND TECHNOLOGY DEVELOPMENT

Purpose To determine the feasibility and desirability of a suggested new system and establish an initial baseline compatibility with NASA’s strategic plans. Develop final mission concept, system-level requirements, needed system technology developments, and program/project technical management plans.

Typical Activities and Their Products

• Review and update documents baselined in Pre-Phase A if needed

• Monitor progress against plans

• Develop and baseline top-level requirements and constraints including internal and external interfaces, integrated logistics and maintenance support, and system software functionality

• Allocate system requirements to functions and to next lower level

• Validate requirements

• Baseline plans

> Systems Engineering Management Plan > Human Systems Integration Plan > Control plans such as the Risk Management Plan, Configuration Management Plan, Data

Management Plan, Safety and Mission Assurance Plan, and Software Development or Management Plan (See NPR 7150.2) > Other crosscutting and specialty plans such as environmental compliance documentation, acquisition surveillance plan, contamination control plan, electromagnetic interference/ electromagnetic compatibility control plan, reliability plan, quality control plan, parts management plan, logistics plan

• Develop preliminary Verification and Validation Plan

• Establish human rating plan and perform initial evaluations

• Develop and baseline mission architecture

> Develop breadboards, engineering units or models identify and reduce high risk concepts > Demonstrate that credible, feasible design(s) exist > Perform and archive trade studies > Initiate studies on human systems interactions

• Initiate environmental evaluation/National Environmental Policy Act process

• Develop initial orbital debris assessment (NASA-STD-8719.14)

• Perform technical management

> Provide technical cost estimate and range and develop system-level cost-effectiveness model > Define the WBS > Develop SOWs > Acquire systems engineering tools and models

(continued)

NASA SYSTEMS ENGINEERING HANDBOOK

24

3.0 NASA Program/Project Life Cycle

> Establish technical resource estimates

• Identify, analyze and update risks

• Perform required Phase A technical activities from NPR 7120.5 as applicable

• Satisfy Phase A reviews’ entrance/success criteria from NPR 7123.1

Reviews

• SRR

• MDR/SDR

solidified, and the project develops more definition

Publication (FIPS PUB) 199. The effort also pro- in the system requirements, top-level system architec-

duces various engineering and management plans to ture, and ConOps. Conceptual designs and analyses

prepare for managing the project’s downstream pro- (including engineering units and physical models, as

cesses such as verification and operations. appropriate) are developed and exhibit more engi- neering detail than in Pre-Phase A. Technical risks are identified in more detail, and technology develop- 3.5 Project Phase B: ment needs become focused. A Systems Engineering Preliminary Design and Management Plan (SEMP) is baselined in Phase A to document how NASA systems engineering require-

Technology Completion

ments and practices of NPR 7123.1 will be addressed

The purpose of Phase B is for the project team to throughout the program life cycle.

complete the technology development, engineering prototyping, heritage hardware and software assess- In Phase A, the effort focuses on allocating func-

ments, and other risk-mitigation activities identified tions to particular items of hardware, software, and

in the project Formulation Agreement (FA) and the to humans. System functional and performance

preliminary design. The project demonstrates that requirements, along with architectures and designs,

its planning, technical, cost, and schedule baselines become firm as system tradeoffs and subsystem

developed during Formulation are complete and con- tradeoffs iterate back and forth, while collaborating

sistent; that the preliminary design complies with its with subject matter experts in the effort to seek out

requirements; that the project is sufficiently mature more cost-effective designs. A method of determin-

to begin Phase C; and that the cost and schedule are ing life cycle cost (i.e., system-level cost-effectiveness

adequate to enable mission success with acceptable model) is refined in order to compare cost impacts

risk. It is at the conclusion of this phase that the for each of the different alternatives. (Trade studies

project and the Agency commit to accomplishing should precede—rather than follow—system design

the project’s objectives for a given cost and schedule. decisions.) Major products to this point include an

For projects with a Life Cycle Cost (LCC) greater accepted functional baseline for the system and its

than $250 million, this commitment is made with major end items. The project team conducts the secu-

the Congress and the U.S. Office of Management rity categorization of IT systems required by NPR

and Budget (OMB). This external commitment is 2810.1 and Federal Information Processing Standard

the Agency Baseline Commitment (ABC). Systems

NASA SYSTEMS ENGINEERING HANDBOOK

25

3.0 NASA Program/Project Life Cycle

SPACE FLIGHT PHASE B: PRELIMINARY DESIGN AND TECHNOLOGY COMPLETION

Purpose To define the project in enough detail to establish an initial baseline capable of meeting mission needs. Develop system structure end product (and enabling product) requirements and generate a preliminary design for each system structure end product.

Typical Activities and Their Products

• Review and update documents baselined in previous phases

• Monitor progress against plans

• Develop the preliminary design

> Identify one or more feasible preliminary designs including internal and external interfaces > Perform analyses of candidate designs and report results > Conduct engineering development tests as needed and report results > Perform human systems integration assessments > Select a preliminary design solution

• Develop operations plans based on matured ConOps

> Define system operations as well as Principal Investigator (PI)/contract proposal management,

review, and access and contingency planning

• Report technology development results

• Update cost range estimate and schedule data (Note that after PDR changes are incorporated and costed, at KDP C this will turn into the Agency Baseline Commitment)

• Improve fidelity of models and prototypes used in evaluations

• Identify and update risks

• Develop appropriate level safety data package and security plan

• Develop preliminary plans

> Orbital Debris Assessment > Decommissioning Plan > Disposal Plan

• Perform required Phase B technical activities from NPR 7120.5 as applicable

• Satisfy Phase B reviews’ entrance/success criteria from NPR 7123.1

Reviews

• PDR

• Safety review

NASA SYSTEMS ENGINEERING HANDBOOK

26

3.0 NASA Program/Project Life Cycle

engineers are involved in this phase to ensure the preliminary designs of the various systems will work together, are compatible, and are likely to meet the customer expectations and applicable requirements.

During Phase B, activities are performed to estab- lish an initial project baseline, which (according to NPR 7120.5 and NPR 7123.1) includes “a formal flow down of the project-level performance require- ments to a complete set of system and subsystem design specifications for both flight and ground ele- ments” and “corresponding preliminary designs.” The technical requirements should be sufficiently detailed to establish firm schedule and cost estimates for the project. It also should be noted, especially for AO-driven projects, that Phase B is where the top- level requirements and the requirements flowed down to the next level are finalized and placed under con- figuration control. While the requirements should be baselined in Phase A, changes resulting from the trade studies and analyses in late Phase A and early Phase B may result in changes or refinement to sys- tem requirements.

It is important in Phase B to validate design decisions against the original goals and objectives and ConOps. All aspects of the life cycle should be considered, including design decisions that affect training, oper- ations resource management, human factors, safety, habitability and environment, and maintainability and supportability.

The Phase B baseline consists of a collection of evolv- ing baselines covering technical and business aspects of the project: system (and subsystem) requirements and specifications, designs, verification and opera- tions plans, and so on in the technical portion of the baseline, and schedules, cost projections, and man- agement plans in the business portion. Establishment of baselines implies the implementation of configura- tion management procedures. (See *Section 6.5*.)

NASA SYSTEMS ENGINEERING HANDBOOK

Phase B culminates in a series of PDRs, containing the system-level PDR and PDRs for lower level end items as appropriate. The PDRs reflect the succes- sive refinement of requirements into designs. Design issues uncovered in the PDRs should be resolved so that final design can begin with unambiguous design-to specifications. From this point on, almost all changes to the baseline are expected to represent successive refinements, not fundamental changes. As noted in FIGURE 2.5-1, significant design changes at and beyond Phase B become increasingly expensive.

3.6 Project Phase C: Final Design and Fabrication

The purpose of Phase C is to complete and docu- ment the detailed design of the system that meets the detailed requirements and to fabricate, code, or otherwise realize the products. During Phase C, activities are performed to establish a complete design (product baseline), fabricate or produce hard- ware, and code software in preparation for integra- tion. Trade studies continue and results are used to validate the design against project goals, objectives, and ConOps. Engineering test units more closely resembling actual hardware are built and tested to establish confidence that the design will function in the expected environments. Human subjects repre- senting the user population participate in operations evaluations of the design, use, maintenance, training procedures, and interfaces. Engineering specialty and crosscutting analysis results are integrated into the design, and the manufacturing process and controls are defined and valid. Systems engineers are involved in this phase to ensure the final detailed designs of the various systems will work together, are compati- ble, and are likely to meet the customer expectations and applicable requirements. During fabrication, the systems engineer is available to answer questions and work any interfacing issues that might arise.

27

3.0 NASA Program/Project Life Cycle

SPACE FLIGHT PHASE C: FINAL DESIGN AND FABRICATION

Purpose To complete the detailed design of the system (and its associated subsystems, including its operations systems), fabricate hardware, and code software. Generate final designs for each system structure end product.

Typical Activities and Their Products

• Review and update documents baselined in previous phases

• Monitor progress against plans

• Develop and document hardware and software detailed designs

> Fully mature and define selected preliminary designs > Add remaining lower level design specifications to the system architecture > Perform and archive trade studies > Perform development testing at the component or subsystem level > Fully document final design and develop data package

• Develop/refine and baseline plans

> Interface definitions > Implementation plans > Integration plans > Verification and validation plans > Operations plans

• Develop/refine preliminary plans

> Decommissioning and disposal plans, including human capital transition > Spares > Communications (including command and telemetry lists)

• Develop/refine procedures for

> Refine integration > Manufacturing and assembly > Verification and validation

• Fabricate (or code) the product

• Identify and update risks

• Monitor project progress against project plans

• Prepare launch site checkout and post launch activation and checkout

• Finalize appropriate level safety data package and updated security plan

• Identify opportunities for preplanned product improvement

• Refine orbital debris assessment

• Perform required Phase C technical activities from NPR 7120.5 as applicable

• Satisfy Phase C review entrance/success criteria from NPR 7123.1

(continued)

NASA SYSTEMS ENGINEERING HANDBOOK

28

3.0 NASA Program/Project Life Cycle

Reviews

• CDR

• PRR

• SIR

• Safety review

All the planning initiated back in Phase A for the testing and operational equipment, processes and analysis, integration of the crosscutting and engineer- ing specialty analysis, and manufacturing processes and controls is implemented. Configuration manage- ment continues to track and control design changes as detailed interfaces are defined. At each step in the successive refinement of the final design, correspond- ing integration and verification activities are planned in greater detail. During this phase, technical param- eters, schedules, and budgets are closely tracked to ensure that undesirable trends (such as an unexpected growth in spacecraft mass or increase in its cost) are recognized early enough to take corrective action. These activities focus on preparing for the CDR, Production Readiness Review (PRR) (if required), and the SIR.

Phase C contains a series of CDRs containing the sys- tem-level CDR and CDRs corresponding to the dif- ferent levels of the system hierarchy. A CDR for each end item should be held prior to the start of fabrica- tion/production for hardware and prior to the start of coding of deliverable software products. Typically, the sequence of CDRs reflects the integration pro- cess that will occur in the next phase; that is, from lower level CDRs to the system-level CDR. Projects, however, should tailor the sequencing of the reviews to meet the needs of the project. If there is a pro- duction run of products, a PRR will be performed to ensure the production plans, facilities, and personnel are ready to begin production. Phase C culminates with an SIR. Training requirements and preliminary

NASA SYSTEMS ENGINEERING HANDBOOK

mission operations procedures are created and base- lined. The final product of this phase is a product ready for integration.

3.7 Project Phase D: System Assembly, Integration and Test, Launch

The purpose of Phase D is to assemble, integrate, ver- ify, validate, and launch the system. These activities focus on preparing for the Flight Readiness Review (FRR)/Mission Readiness Review (MRR). Activities include assembly, integration, verification, and vali- dation of the system, including testing the flight sys- tem to expected environments within margin. Other activities include updating operational procedures, rehearsals and training of operating personnel and crew members, and implementation of the logistics and spares planning. For flight projects, the focus of activities then shifts to prelaunch integration and launch. System engineering is involved in all aspects of this phase including answering questions, provid- ing advice, resolving issues, assessing results of the verification and validation tests, ensuring that the V&V results meet the customer expectations and applicable requirements, and providing information to decision makers for go/no-go decisions.

The planning for Phase D activities was initiated in Phase A. For IT projects, refer to the *IT Systems Engineering Handbook*. The planning for the activ- ities should be performed as early as possible since

29

3.0 NASA Program/Project Life Cycle

SPACE FLIGHT PHASE D: SYSTEM ASSEMBLY, INTEGRATION AND TEST, LAUNCH

Purpose To assemble and integrate the system (hardware, software, and humans), meanwhile developing confidence that it will be able to meet the system requirements. Launch and prepare for operations. Perform system end product implementation, assembly, integration and test, and transition to use.

Typical Activities and Their Products

• Update documents developed and baselined in previous phases

• Monitor project progress against plans

• Identify and update risks

• Integrate/assemble components according to the integration plans

• Perform verification and validation on assemblies according to the V&V Plan and procedures

> Perform system qualification verifications, including environmental verifications > Perform system acceptance verifications and validation(s) (e.g., end-to-end tests encompassing all

elements; i.e., space element, ground system, data processing system) > Assess and approve verification and validation results > Resolve verification and validation discrepancies > Archive documentation for verifications and validations performed > Baseline verification and validation report

• Prepare and baseline

> Operator’s manuals > Maintenance manuals > Operations handbook

• Prepare launch, operations, and ground support sites including training as needed

> Train initial system operators and maintainers > Train on contingency planning > Confirm telemetry validation and ground data processing > Confirm system and support elements are ready for flight > Provide support to the launch and checkout of the system > Perform planned on-orbit operational verification(s) and validation(s)

• Document lessons learned. Perform required Phase D technical activities from NPR 7120.5

• Satisfy Phase D reviews’ entrance/success criteria from NPR 7123.1

Reviews

• Test Readiness Reviews (TRRs)

• System Acceptance Review (SAR) or pre-Ship Review

• ORR

(continued)

NASA SYSTEMS ENGINEERING HANDBOOK

30

3.0 NASA Program/Project Life Cycle

• FRR

• System functional and physical configuration audits

• Safety review

changes at this point can become costly. Phase D concludes with a system that has been shown to be capable of accomplishing the purpose for which it was created.

3.8 Project Phase E: Operations and Sustainment

The purpose of Phase E is to conduct the prime mission to meet the initially identified need and to maintain support for that need. The products of the phase are the results of the mission and performance of the system.

Systems engineering personnel continue to play a role during this phase since integration often overlaps with operations for complex systems. Some programs have repeated operations/flights which require con- figuration changes and new mission objectives with each occurrence. And systems with complex sustain- ment needs or human involvement will likely require evaluation and adjustments that may be beyond the scope of operators to perform. Specialty engineering disciplines, like maintainability and logistics servic- ing, will be performing tasks during this phase as well. Such tasks may require reiteration and/or recur- sion of the common systems engineering processes.

Systems engineering personnel also may be involved in in-flight anomaly resolution. Additionally, soft- ware development may continue well into Phase E. For example, software for a planetary probe may be developed and uplinked while in-flight. Another example would be new hardware developed for space station increments.

NASA SYSTEMS ENGINEERING HANDBOOK

This phase encompasses the evolution of the system only insofar as that evolution does not involve major changes to the system architecture. Changes of that scope constitute new “needs,” and the project life cycle starts over. For large flight projects, there may be an extended period of cruise, orbit insertion, on-orbit assembly, and initial shakedown operations. Near the end of the prime mission, the project may apply for a mission extension to continue mission activities or attempt to perform additional mission objectives.

For additional information on systems engineering in Phase E, see *Appendix T*.

3.9 Project Phase F: Closeout The purpose of Phase F is to implement the systems decommissioning and disposal planning and analyze any returned data and samples. The products of the phase are the results of the mission. The system engi- neer is involved in this phase to ensure all technical information is properly identified and archived, to answer questions, and to resolve issues as they arise.

Phase F deals with the final closeout of the sys- tem when it has completed its mission; the time at which this occurs depends on many factors. For a flight system that returns to Earth after a short mis- sion duration, closeout may require little more than de-integrating the hardware and returning it to its owner. On flight projects of long duration, closeout may proceed according to established plans or may begin as a result of unplanned events, such as fail- ures. Refer to NASA Policy Directive (NPD) 8010.3, Notification of Intent to Decommission or Terminate Operating Space Systems and Terminate Missions,

31

3.0 NASA Program/Project Life Cycle

SPACE FLIGHT PHASE E: OPERATIONS AND SUSTAINMENT

Purpose To conduct the mission and meet the initially identified need and maintain support for that need. Implement the mission operations plan.

Typical Activities and Their Products

• Conduct launch vehicle performance assessment. Commission and activate science instruments

• Conduct the intended prime mission(s)

• Provide sustaining support as planned

> Implement spares plan > Collect engineering and science data > Train replacement operators and maintainers > Train the flight team for future mission phases (e.g., planetary landed operations) > Maintain and approve operations and maintenance logs > Maintain and upgrade the system > Identify and update risks > Address problem/failure reports > Process and analyze mission data > Apply for mission extensions, if warranted

• Prepare for deactivation, disassembly, decommissioning as planned (subject to mission extension)

• Capture lessons learned

• Complete post-flight evaluation reports

• Develop final mission report

• Perform required Phase E technical activities from NPR 7120.5

• Satisfy Phase E reviews’ entrance/success criteria from NPR 7123.1

Reviews

• Post-Launch Assessment Review (PLAR)

• Critical Event Readiness Review (CERR)

• Post-Flight Assessment Review (PFAR) (human space flight only)

• DR

• System upgrade review

• Safety review

NASA SYSTEMS ENGINEERING HANDBOOK

32

3.0 NASA Program/Project Life Cycle

PHASE F: CLOSEOUT

Purpose To implement the systems decommissioning/disposal plan developed in Phase E and perform analyses of the returned data and any returned samples.

Typical Activities and Their Products

• Dispose of the system and supporting processes

• Document lessons learned

• Baseline mission final report

• Archive data

• Capture lessons learned

• Perform required Phase F technical activities from NPR 7120.5

• Satisfy Phase F reviews’ entrance/success criteria from NPR 7123.1

Reviews

• DRR

for terminating an operating mission. Alternatively,

so they are boosted to a higher orbit well beyond the technological advances may make it uneconomical

crowded operational GEO orbit. to continue operating the system either in its current configuration or an improved one.

In addition to uncertainty about when this part of the phase begins, the activities associated with safe To limit space debris, NPR 8715.6, NASA Procedural

closeout of a system may be long and complex and Requirements for Limiting Orbital Debris, provides

may affect the system design. Consequently, different requirements for removing Earth-orbiting robotic

options and strategies should be considered during satellites from their operational orbits at the end of

the project’s earlier phases along with the costs and their useful life. For Low Earth Orbit (LEO) mis-

risks associated with the different options. sions, the satellite is usually deorbited. For small sat- ellites, this is accomplished by allowing the orbit to slowly decay until the satellite eventually burns up

3.10 Funding: The Budget Cycle in Earth’s atmosphere. Larger, more massive satel-

For a description of the NASA Budget Cycle, refer lites and observatories should be designed to demise

to the NASA Expanded Guidance for Systems or deorbit in a controlled manner so that they can

Engineering document found at *https://nen.nasa.gov/* be safely targeted for impact in a remote area of the

*web/se/doc-repository*. See also Section 5.8 of *NASA/* ocean. The Geostationary (GEO) satellites at 35,790

*SP-2014-3705, NASA Space Flight Program and* km above the Earth cannot be practically deorbited,

*Project Management Handbook*.

NASA SYSTEMS ENGINEERING HANDBOOK

33

3.0 NASA Program/Project Life Cycle

3.11 Tailoring and Customization of NPR 7123.1 Requirements In this section, the term *requirements* refers to the “shall” statements imposed from Agency direc- tives. This discussion focuses on the tailoring of the requirements contained in NPR 7123.1.

3.11.1 Introduction NASA policy recognizes the need to accommodate the unique aspects of each program or project to achieve mission success in an efficient and economical man- ner. Tailoring is a process used to accomplish this.

NPR 7123.1 defines *tailoring* as “the process used to seek relief from SE NPR requirements consistent with program or project objectives, allowable risk, and constraints.” Tailoring results in deviations or waivers (see NPR 7120.5, Section 3.5) to SE require- ments and is documented in the next revision of the SEMP (e.g., via the Compliance Matrix).

Since NPR 7123.1 was written to accommodate pro- grams and projects regardless of size or complexity, the NPR requirements leave considerable latitude for interpretation. Therefore, the term “customization” is introduced and is defined as “the modification of recommended SE practices that are used to accom- plish the SE requirements.” Customization does not require waivers or deviations, but significant custom- ization should be documented in the SEMP.

Tailoring and customization are essential systems engineering tools that are an accepted and expected part of establishing the proper SE NPR require- ments for a program or project. Although tailoring is expected for all sizes of projects and programs, small projects present opportunities and challenges that are different from those of large, traditional projects such as the Shuttle, International Space Station, Hubble Space Telescope, and Mars Science Laboratory.

NASA SYSTEMS ENGINEERING HANDBOOK

While the technical aspects of small projects are gen- erally narrower and more focused, they can also be challenging when their objectives are to demonstrate advanced technologies or provide “one of a kind” capabilities. At the same time, their comparatively small budgets and restricted schedules dictate lean and innovative implementation approaches to proj- ect management and systems engineering. Tailoring and customization allow programs and projects to be successful in achieving technical objectives within cost and schedule constraints. The key is effective tai- loring that reflects lessons learned and best practices. Tailoring the SE requirements and customizing the SE best practices to the specific needs of the project helps to obtain the desired benefits while eliminating unnecessary overhead. To accomplish this, an accept- able risk posture must be understood and agreed upon by the project, customer/stakeholder, Center management, and independent reviewers. Even with this foundation, however, the actual process of appro- priately tailoring SE requirements and customizing NPR 7123.1 practices to a specific project can be complicated and arduous. Effective approaches and experienced mentors make the tailoring process for any project more systematic and efficient.

Chapter 6 of the *NASA Software Engineering Handbook* provides guidance on tailoring SE require- ments for software projects.

3.11.2 Criteria for Tailoring NPR 8705.4, Risk Classification for NASA Payloads, is intended for assigning a risk classification to projects and programs. It establishes baseline criteria that enable users to define the risk classification level for NASA payloads on human or non-human-rated launch sys- tems or carrier vehicles. It is also a starting point for understanding and defining criteria for tailoring.

The extent of acceptable tailoring depends on several char- acteristics of the program/project such as the following:

34

3.0 NASA Program/Project Life Cycle

1. Type of mission. For example, the requirements for a human space flight mission are much more rigorous than those for a small robotic mission.

2. Criticality of the mission in meeting the Agency Strategic Plan. Critical missions that absolutely must be successful may not be able to get relief from NPR requirements.

3. Acceptable risk level. If the Agency and the customer are willing to accept a higher risk of failure, some NPR requirements may be waived.

4. National significance. A project that has great national significance may not be able to get relief from NPR requirements.

5. Complexity. Highly complex missions may require more NPR requirements in order to keep systems compatible, whereas simpler ones may not require the same level of rigor.

6. Mission lifetime. Missions with a longer lifetime need to more strictly adhere to NPR require- ments than short-lived programs/projects.

7. Cost of mission. Higher cost missions may require stricter adherence to NPR requirements to ensure proper program/project control.

8. Launch constraints. If there are several launch constraints, a project may need to be more fully compliant with Agency requirements.

3.11.3 Tailoring SE NPR Requirements

Using the Compliance Matrix NPR 7123.1 includes a Compliance Matrix (Appendix H.2) to assist programs and projects in verifying that they meet the specified NPR require- ments. The Compliance Matrix documents the pro- gram/project’s compliance or intent to comply with

NASA SYSTEMS ENGINEERING HANDBOOK

the requirements of the NPR or justification for tai- loring. The Compliance Matrix can be used to assist in identifying where major customization of the way (e.g., formality and rigor) the NPR requirements will be accomplished and to communicate that cus- tomization to the stakeholders. The tailoring pro- cess (which can occur at any time in the program or project’s life cycle) results in deviations or waivers to the NPR requirements depending on the timing of the request. Deviations and waivers of the require- ments can be submitted separately to the Designated Governing Authority or via the Compliance Matrix. The Compliance Matrix is attached to the Systems Engineering Management Plan (SEMP) when sub- mitted for approval. Alternatively, if there is no stand-alone SEMP and the contents of the SEMP are incorporated into another document such as the project plan, the Compliance Matrix can be captured within that plan.

FIGURE 3.11-1 illustrates a notional tailoring process for a space flight project. Project management (such as the project manager/the Principal Investigator/ the task lead, etc.) assembles a project team to tailor the NPR requirements codified in the Compliance Matrix. To properly classify the project, the team (chief engineer, lead systems engineer, safety and mis- sion assurance, etc.) needs to understand the building blocks of the project such as the needs, goals, and objectives as well as the appropriate risk posture.

Through an iterative process, the project team goes through the NPR requirements in the Compliance Matrix to tailor the requirements. A tailoring tool with suggested guidelines may make the tailoring process easier if available. Several NASA Centers including LaRC and MSFC have developed tools for use at their Centers which could be adapted for other Centers. Guidance from Subject Matter Experts (SMEs) should be sought to determine the appropriate amount of tailoring for a specific project.

35

3.0 NASA Program/Project Life Cycle

**Inputs Outputs**

Project

Center-level

**N**

Review/ **Y** Approve

Needs, Goals, Objectives

Program Office

**N**

Engineering/Projects Directorate

**N Y**

Tailoring Tool(s)

PMS&MA

Project Team Review and Refine CETailoring

Approved Compliance Matrix

LSE

Attached to SEMP or Project Plan

FIGURE 3.11-1 Notional Space Flight Products Tailoring Process

3. Scaling the requirement in a manner that bet- ter balances the cost of implementation and the project risk.

Customizing SE practices can include the following:

1. Adjusting the way each of the 17 SE processes is

implemented.

2. Adjusting the formality and timing of reviews.

3.11.4.1 *Non-Applicable NPR Requirements* Each requirement in NPR 7123.1 is assessed for applicability to the individual project or program. For example, if the project is to be developed com- pletely in-house, the requirements of the NPR’s Chapter 4 on contracts would not be applicable. If a system does not contain software, then none of the NPR requirements for developing and maintaining software would be applicable.

NASA SYSTEMS ENGINEERING HANDBOOK

Review/ **Y** Approve

Review/ Approve

Suggest Tailoring

Finalize/ Update Project- Specific Tailoring Risk Posture

and Capture Waiver Rationales

Advisory Teams as Necessary

The Compliance Matrix provides rationales for each of the NPR requirements to assist in understanding. Once the tailoring is finalized and recorded in the Compliance Matrix with appropriate rationales, the requested tailoring proceeds through the appropriate governance model for approval.

3.11.4 Ways to Tailor a SE

Requirement Tailoring often comes in three areas:

1. Eliminating a requirement that does not apply to

the specific program/project.

2. Eliminating a requirement that is overly bur- densome (i.e., when the cost of implementing the requirement adds more risk to the project by diverting resources than the risk of not comply- ing with the requirement).

36

3.0 NASA Program/Project Life Cycle

3.11.4.2 *Adjusting the Scope* Depending on the project or program, some relief on the scope of a requirement may be appropriate. For example, although the governing project management directive (e.g., NPR 7120.5, 7150.2, 7120.7, 7120.8) for a program/project may require certain documents to be standalone, the SE NPR does not require any additional stand-alone documents. For small proj- ects, many of the plans can be described in just a few paragraphs or pages. In these types of projects, any NPR requirements stating that the plans need to be stand-alone document would be too burdensome. In these cases, the information can simply be written and included as part of the project plan or SEMP. If the applicable project management directive (e.g., NPR 7120.5 or NPR 7120.8) requires documents to be stand-alone, a program/project waiver/deviation is needed. However, if there is no requirement or Center expectation for a stand-alone document, a project can customize where that information is recorded and no waiver or deviation is required. Capturing where this information is documented within the systems engi- neering or project management Compliance Matrix would be useful for clarity.

3.11.4.3 *Formality and Timing of Reviews* The governing project management directive iden- tifies the required or recommended life cycle for the specific type of program/project. The life cycle defines the number and timing of the various reviews; however, there is considerable discretion concerning the formality of the review and how to conduct it. NPR 7123.1, Appendix G, provides extensive guidance for suggested review entrance and success criteria. It is expected that the program/ project will customize these criteria in a manner that makes sense for their program/project. The SE NPR does not require a waiver/deviation for this customization; however, departures from review ele- ments required by other NPRs need to be addressed by tailoring those documents.

NASA SYSTEMS ENGINEERING HANDBOOK

If a program/project decides it does not need one of the required reviews, a waiver or deviation is needed. However, the SE NPR does not specify a minimum amount of spacing for these reviews. A small project may decide to combine the SRR and the SDR (or Mission Definition Review (MDR)) for example. As long as the intent for *both* reviews is accomplished, the SE NPR does not require a waiver or deviation. (Note that even though the SE NPR does not require it, a waiver or deviation may still be required in the governing project management NPR.) This customi- zation and/or tailoring should be documented in the Compliance Matrix and/or the review plan or SEMP.

Unless otherwise required by the governing project management directives, the formality of the review can be customized as appropriate for the type of program/project. For large projects, it might be appropriate to conduct a very formal review with a formal Review Item Discrepancy (RID)/Request for Action (RFA) process, a summary, and detailed presentations to a wide audience including boards and pre-boards over several weeks. For small projects, that same review might be done in a few hours across a tabletop with a few stakeholders and with issues and actions simply documented in a word or PowerPoint document.

The NASA Engineering Network Systems Engineering Community of Practice, located at *https://nen.nasa.gov/web/se* includes document tem- plates for milestone review presentations required by the NASA SE process.

3.11.5 Examples of Tailoring and

Customization TABLE 3.11-1 shows an example of the types of mis- sions that can be defined based on a system that breaks projects into various types ranging from a very complex type A to a much simpler type F. When tai- loring a project, the assignment of specific projects to

37

3.0 NASA Program/Project Life Cycle

TABLE 3.11-1 Example of Program/Project Types

Criteria Type A Type B Type C Type D Type E Type F

Description of the

Human Space

Non-Human Types of Mission

Flight or Very

Space Flight or Large Science/

Science/Robotic Robotic Missions

Missions

NASA SYSTEMS ENGINEERING HANDBOOK

Small Science or Robotic Missions

Smaller Science or Technology Missions (ISS payload)

Suborbital or Aircraft or Large Ground based Missions

Aircraft or Ground based technology demonstrations

Priority (Criticality to Agency Strategic Plan) and Acceptable Risk Level

High priority, very low (minimized) risk

High priority, low risk

Medium priority, medium risk

Low priority, high risk

Low priority, high risk

Low to very low priority, high risk

National Significance Very high High Medium Medium to Low Low Very Low

Complexity Very high to high High to Medium Medium to Low Medium to Low Low Low to Very Low

Mission Lifetime (Primary Baseline Mission)

Long. >5 years Medium. 2–5

years

Short. <2 years Short. <2 years N/A N/A

Cost Guidance (estimate LCC)

High (greater than ~$1B)

High to Medium (~$500M–$1B)

Medium to Low (~$100M–$500M)

Low (~$50M–$100M) (~$10–50M) (less than

$10–15M)

Launch Constraints Critical Medium Few Few to none Few to none N/A

Alternative Research Opportunities or Re-flight Opportunities

No alternative or re-flight opportunities

Few or no alternative or re-flight opportunities

Some or few alternative or re-flight opportunities

Significant alternative or re-flight opportunities

Significant alternative or re-flight opportunities

Significant alternative or re-flight opportunities

Achievement of Mission Success Criteria

All practical measures are taken to achieve minimum risk to mission success. The highest assurance standards are used.

Medium or significant risk of not achieving mission success is permitted. Minimal assurance standards are permitted.

Significant risk of not achieving mission success is permitted. Minimal assurance standards are permitted.

Significant risk of not achieving mission success is permitted. Minimal assurance standards are permitted.

Examples HST, Cassini, JIMO, JWST, MPCV, SLS, ISS

Stringent assurance standards with only minor compromises in application to maintain a low risk to mission success.

Medium risk of not achieving mission success may be acceptable. Reduced assurance standards are permitted.

MER, MRO,

ESSP, Explorer

SPARTAN, GAS Discovery

payloads,

Can, technology payloads, ISS

MIDES, ISS

demonstrators, Facility Class

complex subrack

simple ISS, payloads,

payloads, PA-1,

express middeck Attached ISS

ARES 1-X,

and subrack payloads

MEDLI,

payloads, SMEX, CLARREO,

MISSE-X, EV-2 SAGE III, Calipso

IRVE-2, IRVE-3, HiFIRE, HyBoLT, ALHAT, STORRM, Earth Venture I

DAWNAir, InFlame, Research, technology demonstrations

38

3.0 NASA Program/Project Life Cycle

particular types should be viewed as guidance, not as rigid characterization. Many projects will have char- acteristics of multiple types, so the tailoring approach may permit more tailoring for those aspects of the project that are simpler and more open to risk and less tailoring for those aspects of the project where

NASA SYSTEMS ENGINEERING HANDBOOK

complexity and/or risk aversion dominate. These tailoring criteria and definitions of project “types” may vary from Center to Center and from Mission Directorate to Mission Directorate according to what is appropriate for their missions. TABLE 3.11-2 shows an example of how the documentation required of

TABLE 3.11-2 Example of Tailoring NPR 7120 .5 Required Project Products

Type A Type B Type C Type D Type E Type F

Example Project Technical Products

Concept

Fully

Fully

Fully Documentation

Compliant

Compliant

Compliant

(continued) Tailor Tailor Tailor

Mission, Spacecraft, Ground, and Payload Architectures

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor Tailor

Project-Level, System and Subsystem Requirements

Fully Compliant

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor

Design Documentation

Fully Compliant

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor

Operations Concept Fully

Compliant

Fully Compliant

Fully Compliant

Tailor Tailor Tailor

Technology Readiness Assessment Documentation

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor Tailor

Human Systems Integration Plan

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor Tailor

Heritage Assessment Documentation

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor Tailor

Safety Data Packages

Fully Compliant

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor

ELV Payload Safety Process Deliverables

Fully Compliant

Fully Compliant

Fully Compliant

Fully Compliant

Fully Compliant

Not Applicable

Verification and Validation Report

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor Tailor

Operations Handbook

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor Not

Applicable

End of Mission Plans Fully

Compliant

Fully Compliant

Fully Compliant

Tailor Tailor Tailor

Mission Report Fully

Compliant

Fully Compliant

Tailor Tailor Tailor Tailor

39

3.0 NASA Program/Project Life Cycle

Type A Type B Type C Type D Type E Type F

Example Project Plan Control Plans

Risk Management

Fully Plan

Compliant

NASA SYSTEMS ENGINEERING HANDBOOK

Fully Compliant

Fully Compliant

Tailor Tailor Not

Applicable

Technology Development plan

Fully Compliant

Fully Compliant

Fully Compliant

Fully Compliant

Not Applicable

Not Applicable

Systems Engineering Management Plan

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor Tailor

Software Management plan

Fully Compliant

Fully Compliant

Tailor Tailor Tailor Tailor

Verification and Validation Plan

Fully Compliant

Fully Compliant

Tailor Tailor Tailor Tailor

Review Plan Fully

Compliant

Fully Compliant

Fully Compliant

Tailor Tailor Tailor

Integrated Logistics Support Plan

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor Not

Applicable

Science Data Management Plan

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor Not

Applicable

Integration Plan Fully

Compliant

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor

Configuration Management Plan

Fully Compliant

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor

Technology Transfer (formerly Export) Control Plan

Fully Compliant

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor

Lessons Learned Plan

Fully Compliant

Fully Compliant

Fully Compliant

Fully Compliant

Tailor Tailor

Human Rating Certification Package

Fully Compliant

Not Applicable

Not Applicable

Not Applicable

Not Applicable

Not Applicable

a program/project might also be tailored or custom- ized. The general philosophy is that the simpler, less complex projects should require much less documen- tation and fewer formal reviews. Project products should be sensibly scaled.

3.11.6 Approvals for Tailoring Deviations and waivers of the requirements for the SE NPR can be submitted separately to the require- ments owners or in bulk using the appropriate Compliance Matrix found in NPR 7123.1 Appendix

H. If it is a Center that is requesting tailoring of the NPR requirements for standard use at the Center, Appendix H.1 is completed and submitted to the OCE for approval upon request or as changes to the Center processes occur. If a program/project whose responsibility has been delegated to a Center is seek- ing a waiver/deviation from the NPR requirements, the Compliance Matrix in Appendix H.2 is used. In these cases, the Center Director or designee will approve the waiver/deviation.

40

3.0 NASA Program/Project Life Cycle

The result of this tailoring, whether for a Center or

team as well as associated managers. If an indepen- for a program/project, should also be captured in

dent assessment is being conducted on the program/ the next revision of the SEMP along with support-

project, this also allows appropriate modification of ing rationale and documented approvals from the

expectations and assessment criteria. TABLE 3.11-3 requirement owner. This allows communication of

provides some examples of tailoring captured within the approved waivers/deviations to the entire project

the H.2 Compliance Matrix.

TABLE 3.11-3 Example Use of a Compliance Matrix

Req

SE NPR

Requirement

Rationale Req.

Comply? Justification ID

Section

Statement

Owner

SE-05 2.1.5.2 For those

For programs and projects, the

CD Fully requirements

Compliance Matrix in *Appendix*

Compliant owned by Center

*H.2* is filled out showing that the Directors, the

program/project is compliant with technical team

the requirements of this NPR (or a shall complete the

particular Center’s implementation Compliance Matrix

of NPR 7123.1, whichever is in *Appendix H.2*

applicable) or any tailoring thereof and include it in the

is identified and approved by the SEMP.

Center Director or designee as part of the program/project SEMP.

SE-06 2.1.6.1 The DGA shall

CD Fully approve the

Complaint SEMP, waiver authorizations, and other key technical documents to ensure independent assessment of technical content.

SE-24 4.2.1 The NASA technical

team shall define the engineering activities for the periods before contract award, during contract performance, and upon contract completion in the SEMP.

NASA SYSTEMS ENGINEERING HANDBOOK

The DGA, who is often the TA, provides an approval of the SEMPs, waivers to technical requirements and other key technical document to provide assurance of the applicability and technical quality of the products.

It is important for both the

CD Not

Project is government and contractor

Applicable

conducted technical teams to understand

entirely what activities will be handled by

in-house and which organization throughout the

therefore product life cycle. The contractor(s)

there are no will typically develop a SEMP or its

contracts equivalent to describe the technical

involved activities in their portion of the project, but an overarching SEMP is needed that will describe all technical activities across the life cycle whether contracted or not.

41

3.0 NASA Program/Project Life Cycle

NASA SYSTEMS ENGINEERING HANDBOOK

42

4.0 System Design Processes

This design chapter processes describes listed the in FIGURE activities 2.1-1. in the The system chap- ter is separated into sections corresponding to pro- cesses 1 to 4 listed in FIGURE 2.1-1. The tasks within each process are discussed in terms of inputs, activ- ities, and outputs. Additional guidance is provided using examples that are relevant to NASA projects.

The system design processes are interdependent, highly iterative and recursive processes resulting in a validated set of requirements and a design solution that satisfies a set of stakeholder expectations. There are four system design processes: developing stake- holder expectations, technical requirements, logical decompositions, and design solutions.

FIGURE 4.0-1 illustrates the recursive relationship among the four system design processes. These pro- cesses start with a study team collecting and clarifying the stakeholder expectations, including the mission objectives, constraints, design drivers, operational objectives, and criteria for defining mission success. This set of stakeholder expectations and high-level requirements is used to drive an iterative design loop where a straw man architecture/design, the concept of operations, and derived requirements are devel- oped. These three products should be consistent with

each other and will require iterations and design deci- sions to achieve this consistency. Once consistency is achieved, analyses allow the project team to validate the proposed design against the stakeholder expecta- tions. A simplified validation asks the questions: Will the system work as expected? Is the system achiev- able within budget and schedule constraints? Does the system provide the functionality and fulfill the operational needs that drove the project’s funding approval? If the answer to any of these questions is no, then changes to the design or stakeholder expec- tations will be required, and the process starts again. This process continues until the system—architec- ture, ConOps, and requirements—meets the stake- holder expectations.

The depth of the design effort should be sufficient to allow analytical verification of the design to the requirements. The design should be feasible and cred- ible when judged by a knowledgeable independent review team and should have sufficient depth to sup- port cost modeling and operational assessment.

Once the system meets the stakeholder expectations, the study team baselines the products and prepares for the next phase. Often, intermediate levels of decomposition are validated as part of the process. In

43 NASA SYSTEMS ENGINEERING HANDBOOK

4.0 System Design Processes

Iterate ConOps

Iterate Requirements Iterate Expectations

Stakeholder Expectations

Requirements Definition Inconsistencies - Iterate

Needs,

No - Iterate Goals and Objectives

Program Authority

Constraints

Good Yes

Success Criteria

Design Solution Definition

Evaluate Compare NASA SYSTEMS ENGINEERING HANDBOOK

**Derived and Allocated Requirements**

Develop ConOps

•Functional

•Performance

•Interface

•Operational

•Safety

•“ilities”

Validate

Req. Meet Req. Set

ConOps?

No – Recursive Cycle

Logical Decomposition

**Decomposition** To Product Realization Processes

Iterate

Lowest Level?

Success Criteria

Develop Design

•Functional Flow

•Temporal Flow

•Behavioral

•Data Flow

•States and Modes

ConOps

FIGURE 4.0-1 Interrelationships among the System Design Processes

SYSTEM DESIGN KEYS

• Successfully understanding and defining the mission objectives and the concept of operations are keys to capturing the stakeholder expectations, which will translate into quality requirements and operational efficiencies over the life cycle of the project.

• Complete and thorough requirements traceability is a critical factor in successful validation of requirements.

• Clear and unambiguous requirements will help avoid misunderstanding when developing the overall system and when making major or minor changes.

• Document all decisions made during the development of the original design concept in the technical data package. This will make the original design philosophy and negotiation results available to assess future proposed changes and modifications against.

• The validation of a design solution is a continuing recursive and iterative process during which the design solution is evaluated against stakeholder expectations.

Develop Architecture

44

4.0 System Design Processes

the next level of decomposition, the baselined derived (and allocated) requirements become the set of high- level requirements for the decomposed elements and the process begins again. These system design pro- cesses are primarily applied in Pre-Phase A and con- tinue through Phase C.

The system design processes during Pre-Phase A focus on producing a feasible design that will lead to Formulation approval. During Phase A, alterna- tive designs and additional analytical maturity are pursued to optimize the design architecture. Phase B results in a preliminary design that satisfies the approval criteria. During Phase C, detailed, build-to designs are completed.

This is a simplified description intended to demon- strate the recursive relationship among the system design processes. These processes should be used as guidance and tailored for each study team depending on the size of the project and the hierarchical level of the study team. The next sections describe each of the four system design processes and their associated products for a given NASA mission.

4.1 Stakeholder Expectations Definition

The Stakeholder Expectations Definition Process is the initial process within the SE engine that estab- lishes the foundation from which the system is designed and the product is realized. The main pur- pose of this process is to identify who the stakehold- ers are and how they intend to use the product. This is usually accomplished through use-case scenarios (sometimes referred to as Design Reference Missions (DRMs)) and the ConOps.

NASA SYSTEMS ENGINEERING HANDBOOK

4.1.1 Process Description FIGURE 4.1-1 provides a typical flow diagram for the Stakeholder Expectations Definition Process and identifies typical inputs, outputs, and activities to consider in defining stakeholder expectations.

4.1.1.1 *Inputs* Typical inputs needed for the Stakeholder Expectations Definition Process include the following:

• Initial Customer Expectations: These are the needs, goals, objectives, desires, capabilities, and other constraints that are received from the cus- tomer for the product within the product layer. For the top-tier products (final end item), these are the expectations of the originating customer who requested the product. For an end product within the product layer, these are the expectations of the recipient of the end item when transitioned.

• Other Stakeholder Expectations: These are the expectations of key stakeholders other than the customer. For example, such stakeholders may be the test team that will be receiving the transi- tioned product (end product and enabling prod- ucts) or the trainers that will be instructing the operators or managers that are accountable for the product at this layer.

• Customer Flow-down Requirements: These are any requirements that are being flowed down or allocated from a higher level (i.e., parent require- ments). They are helpful in establishing the expec- tations of the customer at this layer.

4.1.1.2 *Process Activities* 4.1.1.2.1 ***Identify Stakeholders*** A “stakeholder” is a group or individual that is affected by or has a stake in the product or project. The key players for a project/product are called the key stakeholders. One key stakeholder is always the

45

4.0 System Design Processes

NASA SYSTEMS ENGINEERING HANDBOOK

*To* Technical Requirements Definition and Establish list of stakeholders

Requirements and Interface Management Processes

*From* Project

Elicit stakeholder expectations

Validated Stakeholder Expectations

Initial Customer Expectations

Establish operations concept and support strategies

*To* Technical Requirements Definition and Configuration Define stakeholder expectations in acceptable

Management Processes Other Stakeholder

statements Expectations

Concept of Operations

Analyze expectation statements for measures of effectiveness

Enabling Product Validate that defined expectation statements

Support Strategies reflect bidirectional traceability Customer Flow-down Requirements

*To* Technical Requirements Obtain stakeholder commitments to the

Definition and Technical Data validated set of expectations

Management Processes

Baseline stakeholder expectations

Measures of Effectiveness

Capture work products from stakeholder expectations activities

FIGURE 4.1-1 Stakeholder Expectations Definition Process

“customer.” The customer may vary depending on where the systems engineer is working in the PBS. For example, at the topmost level, the customer may be the person or organization that is purchasing the product. For a systems engineer working three or four levels down in the PBS, the customer may be the leader of the team that takes the element and inte- grates it into a larger assembly. Regardless of where the systems engineer is working within the PBS, it is important to understand what is expected by the customer.

Other interested parties are those who affect the project by providing broad, overarching constraints within which the customers’ needs should be

achieved. These parties may be affected by the result- ing product, the manner in which the product is used, or have a responsibility for providing life cycle support services. Examples include Congress, advi- sory planning teams, program managers, maintain- ers, and mission partners. It is important that the list of stakeholders be identified early in the process, as well as the primary stakeholders who will have the most significant influence over the project.

The customer and users of the system are usually easy to identify. The other key stakeholders may be more difficult to identify and they may change depending on the type of the project and the phase the project is in. TABLE 4.1-1 provides some

46

4.0 System Design Processes

TABLE 4.1-1 Stakeholder Identification throughout the Life Cycle

Life-Cycle Stage Example Stakeholders

Pre-Phase A NASA Headquarters, NASA Centers, Presidential Directives, NASA advisory committees, the

National Academy of Sciences

Phase A Mission Directorate, customer, potential users, engineering disciplines, safety organization

Phase B Customer, engineering disciplines, safety, crew, operations, logistics, production facilities,

suppliers, principle investigators

Phase C Customer, engineering disciplines, safety, crew, operations, logistics, production facilities,

suppliers, principle investigators

Phase D Customer, engineering disciplines, safety, crew, operations, training, logistics, verification team,

Flight Readiness Board members

Phase E Customer, system managers, operations, safety, logistics, sustaining team, crew, principle

investigators, users

Phase F Customer, NASA Headquarters, operators, safety, planetary protection, public

examples of stakeholders in the life cycle phase that

encompass expenditures (resources), time to deliver, should be considered.

life cycle support expectations, performance objec- tives, operational constraints, training goals, or other 4.1.1.2.2 ***Understand Stakeholder Expectations***

less obvious quantities such as organizational needs Thoroughly understanding the customer and other

or geopolitical goals. This information is reviewed, key stakeholders’ expectations for the project/prod-

summarized, and documented so that all parties can uct is one of the most important steps in the systems

come to an agreement on the expectations. engineering process. It provides the foundation upon which all other systems engineering work depends. It

FIGURE 4.1-2 shows the type of information needed helps ensure that all parties are on the same page and

when defining stakeholder expectations and depicts that the product being provided will satisfy the cus-

how the information evolves into a set of high-level tomer. When the customer, other stakeholders, and

requirements. The yellow lines depict validation the systems engineer mutually agree on the func-

paths. Examples of the types of information that tions, characteristics, behaviors, appearance, and

would be defined during each step are also provided. performance the product will exhibit, it sets more realistic expectations on the customer’s part and

Defining stakeholder expectations begins with helps prevent significant requirements creep later in

the *mission authority* and *strategic objectives* that the life cycle.

the mission is meant to achieve. Mission authority changes depending on the category of the mission. Through interviews/discussions, surveys, marketing

For example, science missions are usually driven by groups, e-mails, a Statement of Work (SOW), an

NASA Science Mission Directorate strategic plans, initial set of customer requirements, or some other

whereas the exploration missions may be driven by a means, stakeholders specify what is desired as an end

Presidential directive. Understanding the objectives state or as an item to be produced and put bounds

of the mission helps ensure that the project team is on the achievement of the goals. These bounds may

working toward a common vision. These goals and

NASA SYSTEMS ENGINEERING HANDBOOK

47

4.0 System Design Processes

**Mission**

**Mission**

**Operational Goals**

**Objectives**

**Objectives**

**Operational Drivers Measurements Mission Drivers**

**Explorations**

NASA SYSTEMS ENGINEERING HANDBOOK

**Success Criteria**

**Design Drivers**

• Agency Strategic Plans

• Announcements of Opportunity

• Road Maps

• Directed Missions

• Science Objectives

• Exploration Objectives

• Technology Demonstration Objectives

• Technology Development Objectives

• Programmatic Objectives

• Integration and Test

• Launch

• On-Orbit

• Transfer

• Surface

• Science Data Distribution

• Maintenance

• Logistics

• Etc.

• What

• Launch Date measurements?

• Mission Duration

• How well?

• Orbit

• Cost Constraints

• Etc.

• What explorations?

• What goals?

FIGURE 4.1-2 Information Flow for Stakeholder Expectations

objectives form the basis for developing the mission,

In identifying the full set of expectations, the systems so they need to be clearly defined and articulated.

engineer will need to interact with various commu- nities, such as those working in the areas of orbital The project team should also identify the *constraints*

debris, space asset protection, human systems inte- that may apply. A “constraint” is a condition that is to

gration, quality assurance, and reliability. Ensuring be met. Sometimes a constraint is dictated by external

that a complete set of expectations is captured will factors such as orbital mechanics, an existing system

help prevent “surprise” features from arising later in that must be utilized (external interface), a regu-

the life cycle. For example, space asset protection may latory restriction, or the state of technology; some-

require additional encryption for the forward link times constraints are the result of the overall budget

commands, additional shielding or filtering for RF environment. Concepts of operation and constraints

systems, use of a different frequency, or other design also need to be included in defining the stakeholder

changes that might be costly to add to a system that expectations. These identify how the system should

has already been developed. be operated to achieve the mission objectives.

4.1.1.2.3 ***Identify Needs, Goals, and Objectives*** In order to define the goals and objectives, it is nec- NOTE: It is extremely important to involve stake-

essary to elicit the needs, wants, desires, capabilities, holders in all phases of a project. Such involvement

external interfaces, assumptions, and constraints should be built in as a self-correcting feedback loop

from the stakeholders. Arriving at an agreed-to set of that will significantly enhance the chances of mis-

goals and objectives can be a long and arduous task. sion success. Involving stakeholders in a project

Proactive iteration with the stakeholders throughout builds confidence in the end product and serves as a

the systems engineering process is the way that all par- validation and acceptance with the target audience.

ties can come to a true understanding of what should be done and what it takes to do the job. It is important

48

4.0 System Design Processes

to know who the primary stakeholders are and who has the decision authority to help resolve conflicts.

Needs, Goals, and Objectives (NGOs) provide a mechanism to ensure that everyone (implementer, customer, and other stakeholders) is in agreement at the beginning of a project in terms of defining the problem that needs to be solved and its scope. NGOs are not contractual requirements or designs.

Needs are defined in the answer to the question “What problem are we trying to solve?” Goals address what must be done to meet the needs; i.e., what the customer wants the system to do. Objectives expand on the goals and provide a means to docu- ment specific expectations. (Rationale should be pro- vided where needed to explain why the need, goal, or objective exists, any assumptions made, and any other information useful in understanding or man- aging the NGO.)

Well-written NGOs provide clear traceability from the needs, then to the goals, and then to objectives. For example, if a given goal does not support a need, or an objective does not support a goal, it should not be part of the integrated set of NGOs. This traceabil- ity helps ensure that the team is actually providing what is needed.

The following definitions (source: *Applied Space Systems Engineering* edited by Larson, Kirkpatrick, Sellers, Thomas, and Verma) are provided to help the reader interpret the NGOs contained in this product.

• Need: A single statement that drives everything else. It should relate to the problem that the system is supposed to solve but not be the solution. The need statement is singular. Trying to satisfy more than one need requires a trade between the two, which could easily result in failing to meet at least one, and possibly several, stakeholder expectations.

NASA SYSTEMS ENGINEERING HANDBOOK

• Goals: An elaboration of the need, which con- stitutes a specific set of expectations for the sys- tem. Goals address the critical issues identified during the problem assessment. Goals need not be in a quantitative or measurable form, but they should allow us to assess whether the system has achieved them.

• Objectives: Specific target levels of outputs the system must achieve. Each objective should relate to a particular goal. Generally, objectives should meet four criteria. (1) They should be specific enough to provide clear direction, so developers, customers, and testers will understand them. They should aim at results and reflect what the system needs to do but not outline how to implement the solution. (2) They should be measurable, quantifi- able, and verifiable. The project needs to monitor the system’s success in achieving each objective. (3) They should be aggressive but attainable, challenging but reachable, and targets need to be realistic. Objectives “To Be Determined” (TBD) may be included until trade studies occur, oper- ations concepts solidify, or technology matures. Objectives need to be feasible before require- ments are written and systems designed. (4) They should be results-oriented focusing on desired outputs and outcomes, not on the methods used to achieve the target (what, not how). It is import- ant to always remember that objectives are not requirements. Objectives are identified during pre-Phase A development and help with the even- tual formulation of a requirements set, but it is the requirements themselves that are contractually binding and will be verified against the “as-built” system design.

These stakeholder expectations are captured and are considered as initial until they can be further refined through development of the concept of operations and final agreement by the stakeholders.

49

4.0 System Design Processes

4.1.1.2.4 ***Establish Concept of Operations and Support***

***Strategies*** After the initial stakeholder expectations have been established, the development of a Concept of Operations (ConOps) will further ensure that the technical team fully understands the expectations and how they may be satisfied by the product, and that understanding has been agreed to by the stake- holders. This may lead to further refinement of the initial set of stakeholder expectations if gaps or ambig- uous statements are discovered. These scenarios and concepts of how the system will behave provide an implementation-free understanding of the stakehold- ers’ expectations by defining what is expected with- out addressing how (the design) to satisfy the need. It captures required behavioral characteristics and the manner in which people will interact with the system. Support strategies include provisions for fab- rication, test, deployment, operations, sustainment, and disposal.

The ConOps is an important component in captur- ing stakeholder expectations and is used in defin- ing requirements and the architecture of a project. It stimulates the development of the requirements and architecture related to the user elements of the system. It serves as the basis for subsequent defini- tion documents such as the operations plan, launch and early orbit plan, and operations handbook, and it provides the foundation for the long-range opera- tional planning activities such as operational facili- ties, staffing, and network scheduling.

The ConOps is an important driver in the system requirements and therefore should be considered early in the system design processes. Thinking through the ConOps and use cases often reveals requirements and design functions that might otherwise be overlooked. For example, adding system requirements to allow for communication during a particular phase of a mis- sion may require an additional antenna in a specific

NASA SYSTEMS ENGINEERING HANDBOOK

location that may not be required during the nominal mission. The ConOps should include scenarios for all significant operational situations, including known off-nominal situations. To develop a useful and complete set of scenarios, important malfunctions and degraded-mode operational situations should be considered. The ConOps is also an important aide to characterizing life cycle staffing goals and function allocation between humans and systems. In walking through the accomplishment of mission objectives, it should become clear when decisions need to be made as to what the human operators are contributing vs. what the systems are responsible for delivering.

The ConOps should consider all aspects of opera- tions including nominal and off-nominal operations during integration, test, and launch through dis- posal. Typical information contained in the ConOps includes a description of the major phases; operation timelines; operational scenarios and/or DRM (see FIGURE 4.1-3 for an example of a DRM); fault man- agement strategies, description of human interaction and required training, end-to-end communications strategy; command and data architecture; opera- tional facilities; integrated logistic support (resup- ply, maintenance, and assembly); staffing levels and required skill sets; and critical events. The operational scenarios describe the dynamic view of the systems’ operations and include how the system is perceived to function throughout the various modes and mode transitions, including interactions with external inter- faces, response to anticipated hazard and faults, and during failure mitigations. For exploration missions, multiple DRMs make up a ConOps. The design and performance analysis leading to the requirements should satisfy all of them.

Additional information on the development of the ConOps is discussed in Section 4.1.2.1 of the NASA Expanded Guidance for Systems Engineering docu- ment found *https://nen.nasa.gov/web/se/doc-repository*.

50

4.0 System Design Processes

CONCEPT OF OPERATIONS VS. OPERATIONS CONCEPT

Concept of Operations Developed early in Pre-Phase A by the technical team, describes the overall high-level concept of how the system will be used to meet stakeholder expectations, usually in a time sequenced manner. It describes the system from an operational perspective and helps facilitate an understanding of the system goals. It stimulates the development of the requirements and architecture related to the user elements of the system. It serves as the basis for subsequent definition documents and provides the foundation for the long-range operational planning activities.

Operations Concept A description of how the flight system and the ground system are used together to ensure that the concept of operation is reasonable. This might include how mission data of interest, such as engineering or scientific data, are captured, returned to Earth, processed, made available to users, and archived for future reference. It is typically developed by the operational team. (See NPR 7120.5.)

NASA SYSTEMS ENGINEERING HANDBOOK

Moon

Ascent Stage LSAM Performs Lunar Orbit Injection

Expended

100 km Low Lunar Orbit

Earth Departure Stage Expended

Low Earth Orbit

Lunar Surface Access Module

Direct or Skip (LSAM) Crew Exploration Vehicle

Land Entry

Earth Departure Stage Earth

FIGURE 4.1-3 Example of a Lunar Sortie DRM Early in the Life Cycle

51

4.0 System Design Processes

*Appendix S* contains one possible outline for developing a ConOps. The specific sections of the ConOps will vary depending on the scope and purpose of the project.

4.1.1.2.5 ***Define Stakeholder Expectations in***

***Acceptable Statements*** Once the ConOps has been developed, any gaps or ambiguities have been resolved, and understanding between the technical team and stakeholders about what is expected/intended for the system/product has been achieved, the expectations can be formally doc- umented. This often comes in the form of NGOs, mission success criteria, and design drivers. These may be captured in a document, spreadsheet, model, or other form appropriate to the product.

The *design drivers* will be strongly dependent upon the ConOps, including the operational environment, orbit, and mission duration requirements. For science missions, the design drivers include, at a minimum, the mission launch date, duration, and orbit, as well as operational considerations. If alternative orbits are to be considered, a separate concept is needed for each orbit. Exploration missions should consider the destination, duration, operational sequence (and sys- tem configuration changes), crew interactions, main- tenance and repair activities, required training, and in situ exploration activities that allow the explora- tion to succeed.

4.1.1.2.6 ***Analyze Expectations Statements for Measures***

***of Effectiveness*** The *mission success criteria* define what the mission needs to accomplish to be successful. This could be in the form of science missions, exploration concept for human exploration missions, or a technological goal for technology demonstration missions. The success criteria also define how well the concept measurements or exploration activities should be accomplished. The success criteria capture the stake- holder expectations and, along with programmatic

NASA SYSTEMS ENGINEERING HANDBOOK

requirements and constraints, are used within the high-level requirements.

Measures of Effectiveness (MOEs) are the measures of success that are designed to correspond to accom- plishment of the system objectives as defined by the stakeholder’s expectations. They are stated from the stakeholder’s point of view and represent criteria that are to be met in order for the stakeholder to consider the project successful. As such, they can be synon- ymous with mission/project success criteria. MOEs are developed when the NGOs or other stakeholder expectation documentation is developed. Additional information on MOEs is contained in Section 6.7.2.4 of the NASA Expanded Guidance for SE document at *https://nen.nasa.gov/web/se/doc-repository*.

4.1.1.2.7 ***Validate That Defined Expectation Statements***

***Reflect Bidirectional Traceability*** The NGOs or other stakeholder expectation doc- umentation should also capture the source of the expectation. Depending on the location within the product layer, the expectation may be traced to an NGO or a requirement of a higher layer product, to organizational strategic plans, or other sources. Later functions and requirements will be traced to these NGOs. The use of a requirements management tool or model or other application is particularly useful in capturing and tracing expectations and requirements.

4.1.1.2.8 ***Obtain Stakeholder Commitments to the***

***Validated Set of Expectations*** Once the stakeholder and the technical team are in agreement with the expressed stakeholder expec- tations and the concept of operations, signatures or other forms of commitment are obtained. In order to obtain these commitments, a concept review is typi- cally held on a formal or informal basis depending on the scope and complexity of the system (see *Section 6.7*). The stakeholder expectations (e.g., NGOs), MOEs, and concept of operations are presented, discussed, and refined as necessary to achieve final

52

4.0 System Design Processes

agreement. This agreement shows that both sides have committed to the development of this product.

4.1.1.2.9 ***Baseline Stakeholder Expectations*** The set of stakeholder expectations (e.g., NGOs and MOEs) and the concept of operations that are agreed upon are now baselined. Any further changes will be required to go through a formal or informal (depending on the nature of the product) approval process involving both the stakeholder and the technical team.

4.1.1.2.10 ***Capture Work Products*** In addition to developing, documenting, and base- lining stakeholder expectations, the ConOps and MOEs discussed above and other work products from this process should be captured. These may include key decisions made, supporting decision rationale and assumptions, and lessons learned in performing these activities.

4.1.1.3 *Outputs* Typical outputs for capturing stakeholder expecta- tions include the following:

• Validated Stakeholder Expectations: These are the agreed-to set of expectations for this product layer. They are typically captured in the form of needs, goals, and objectives with constraints and assumptions identified. They may also be in the form of models or other graphical forms.

• Concept of Operations: The ConOps describes how the system will be operated during the life cycle phases that will meet stakeholder expecta- tions. It describes the system characteristics from an operational perspective and helps facilitate an understanding of the system goals and objectives and other stakeholder expectations. Examples would be the ConOps document, model, or a Design Reference Mission (DRM).

NASA SYSTEMS ENGINEERING HANDBOOK

• Enabling Product Support Strategies: These include any special provisions that might be needed for fabrication, test, deployment, opera- tions sustainment, and disposal of the end prod- uct. They identify what support will be needed and any enabling products that will need to be developed in order to generate the end product.

• Measures of Effectiveness: A set of MOEs is developed based on the stakeholder expectations. These are measures that represent expectations that are critical to the success of the system, and failure to satisfy these measures will cause the stakeholder to deem the system unacceptable.

Other outputs that might be generated:

• Human/Systems Function Allocation: This describes the interaction of the hardware and software systems with all personnel and their supporting infrastructure. In many designs (e.g., human space flight) human operators are a critical total-system component and the roles and respon- sibilities of the humans-in-the-system should be clearly understood. This should include all human/system interactions required for a mission including assembly, ground operations, logistics, in-flight and ground maintenance, in-flight oper- ations, etc.

4.1.2 Stakeholder Expectations Definition Guidance Refer to Section 4.1.2 in the NASA Expanded Guidance for Systems Engineering at *https://nen. nasa.gov/web/se/doc-repository* for additional guid- ance on:

• Concept of Operations (including examples),

• protection of space assets, and

• identification of stakeholders for each phase.

53

4.0 System Design Processes

4.2 Technical Requirements Definition The Technical Requirements Definition Process transforms the stakeholder expectations into a defi- nition of the problem and then into a complete set of validated technical requirements expressed as “shall” statements that can be used for defining a design solution for the Product Breakdown Structure (PBS) and related enabling products. The process of requirements definition is a recursive and iterative one that develops the stakeholders’ requirements, prod- uct requirements, and lower level product/compo- nent requirements. The requirements should enable the description of all inputs, outputs, and required relationships between inputs and outputs, including constraints, and system interactions with operators, maintainers, and other systems. The requirements documents organize and communicate requirements to the customer and other stakeholders and the tech- nical community.

NOTE: It is important to note that the team must not rely solely on the requirements received to design and build the system. Communication and iteration with the relevant stakeholders are essential to ensure a mutual understanding of each require- ment. Otherwise, the designers run the risk of misunderstanding and implementing an unwanted solution to a different interpretation of the require- ments. This iterative stakeholder communication is a critically important part of project validation. Always confirm that the right products and results are being developed.

Technical requirements definition activities apply to the definition of all technical requirements from the program, project, and system levels down to the low- est level product/component requirements document.

NASA SYSTEMS ENGINEERING HANDBOOK

4.2.1 Process Description FIGURE 4.2-1 provides a typical flow diagram for the Technical Requirements Definition Process and iden- tifies typical inputs, outputs, and activities to con- sider in addressing technical requirements definition.

4.2.1.1 *Inputs* Typical inputs needed for the requirements process include the following:

• Baselined Stakeholder Expectations: This is the agreed-to set of stakeholder expectations (e.g., needs, goals, objectives, assumptions, constraints, external interfaces) for the product(s) of this prod- uct layer.

• Baselined Concept of Operations: This describes how the system will be operated during the life cycle phases to meet stakeholder expectations. It describes the system characteristics from an oper- ational perspective and helps facilitate an under- standing of the system goals, objectives, and constraints. It includes scenarios, use cases, and/or Design Reference Missions (DRMs) as appropriate for the project. It may be in the form of a docu- ment, graphics, videos, models, and/or simulations.

• Baselined Enabling Support Strategies: These describe the enabling products that were identi- fied in the Stakeholder Expectations Definition Process as needed to develop, test, produce, operate, or dispose of the end product. They also include descriptions of how the end product will be supported throughout the life cycle.

• Measures of Effectiveness: These MOEs were identified during the Stakeholder Expectations Definition Process as measures that the stake- holders deemed necessary to meet in order for the project to be considered a success (i.e., to meet success criteria).

54

4.0 System Design Processes

Analyze scope of problem

*From* **Stakeholder Expectations Definition** and **Configuration Management Processes**

Define design and product constraints

Define technical require- ments in acceptable “shall” statements

Define measures of

Define technical

NASA SYSTEMS ENGINEERING HANDBOOK

Define functional and behavioral expectation in technical terms

*To* **Logical Decomposition** and **Requirements** and **Interface Management** Baselined Stakeholder **Processes**

Expectations Define performance

requirements for each

Validated Technical Requirements

Baselined Concept of

defined functional and Operations

behavioral expectation

Measures of Performance

Measures of Effectiveness

Validate technical requirements

Establish technical requirements baseline

performance measures

*To* **Logical Decomposition** and **Technical Data Management Processes** Baselined Enabling Support Strategies

*To* **Technical Assessment Process**

Technical Performance

performance for each

Measures

measure of effectiveness

Capture work products from technical requirements definition activities

FIGURE 4.2-1 Technical Requirements Definition Process

Other inputs that might be useful in determining the

4.2.1.2 *Process Activities* technical requirements:

4.2.1.2.1 ***Define Constraints, Functional and***

***Behavioral Expectations***

• Human/Systems Function Allocation: This

The top-level requirements and expectations are ini- describes the interaction of the hardware and

tially assessed to understand the technical problem software systems with all personnel and their sup-

to be solved (scope of the problem) and establish the porting infrastructure. When human operators

design boundary. This boundary is typically estab- are a critical total-system component, the roles

lished by performing the following activities: and responsibilities of the humans-in-the-system should be clearly understood. This should include

• Defining constraints that the design needs to all human/system interactions required for a mis-

adhere to or that limit how the system will be sion including assembly, ground operations, logis-

used. The constraints typically cannot be changed tics, in-flight and ground maintenance, in-flight

based on trade-off analyses. operations, etc.

• Identifying those elements that are already under design control and cannot be changed. This helps

55

4.0 System Design Processes

establish those areas where further trades will be

interaction requirements). Crosscutting require- made to narrow potential design solutions.

ments include environmental, safety, human factors, and those that originate from the “-ilities” and from

• Identifying external and enabling systems with

Design and Construction (D&C) standards. FIGURE which the system should interact and establishing

4.2-2 is a general overview on the flow of require- physical and functional interfaces (e.g., mechani-

ments, what they are called, and who is responsible cal, electrical, thermal, human, etc.).

(owns) for approving waivers.

• Defining functional and behavioral expectations for the range of anticipated uses of the system as

• Functional requirements define what identified in the ConOps. The ConOps describes

functions need to be performed to how the system will be operated and the possible

accomplish the objectives. use-case scenarios.

• Performance requirements define how well the system needs to perform the functions. 4.2.1.2.2 ***Define Requirements*** A complete set of project requirements includes those that are decomposed and allocated down to design

With an overall understanding of the constraints, elements through the PBS and those that cut across

physical/functional interfaces, and functional/behav- product boundaries. Requirements allocated to the

ioral expectations, the requirements can be further PBS can be functional requirements (what functions

defined by establishing performance and other tech- need to be performed), performance requirements

nical criteria. The expected performance is expressed (how well these functions should be performed),

as a quantitative measure to indicate how well each and interface requirements (product to product

product function needs to be accomplished.

EXAMPLE OF FUNCTIONAL AND PERFORMANCE REQUIREMENTS

Initial Function Statement The Thrust Vector Controller (TVC) shall provide vehicle control about the pitch and yaw axes.

This statement describes a high-level function that the TVC must perform. The technical team needs to transform this statement into a set of design-to functional and performance requirements.

Functional Requirements with Associated Performance Requirements

• The TVC shall gimbal the engine a maximum of 9 degrees, ± 0.1 degree.

• The TVC shall gimbal the engine at a maximum rate of 5 degrees/second ± 0.3 degrees/second.

• The TVC shall provide a force of 40,000 pounds, ± 500 pounds.

• The TVC shall have a frequency response of 20 Hz, ± 0.1 Hz.

NASA SYSTEMS ENGINEERING HANDBOOK

56

4.0 System Design Processes

**Flow Type Ownership** Mission Directorate Imposed Requirements

Ex: At least one major

Program

element shall be provided by the international community. Imposed Requirements

Ex: The spacecraft shall provide a direct Earth entry capability for 11500 m/s or greater.

NASA SYSTEMS ENGINEERING HANDBOOK

**Owned** Self-Imposed

Derived

**“Programmatic”**

All **Requirements**

**by Program/ Project** Requirements

Self-Imposed Derived Requirements

**Technical Requirements**

See note\*

**Owned by Technical Authority**

Likewise flow to Lower Level Systems

**Program Requirements**

**Project Requirements**

Ex: The spacecraft shall provide a direct Earth entry capability for 11500 m/s or greater.

Ex: The system shall have a 1.4 factor of safety

\* Requirements invoked by OCE, OSMA and OCHMO directives, technical standards and Center institutional requirements

FIGURE 4.2-2 Flow, Type and Ownership of Requirements

NOTE: Requirements can be generated from

technical requirements from which the system will non-obvious stakeholders and may not directly

be architected and designed. FIGURE 4.2-3 shows an support the current mission and its objectives, but

example of parent and child requirement flowdown. instead provide an opportunity to gain additional benefits or information that can support the Agency

4.2.1.2.3 ***Define Requirements in Acceptable*** or the Nation. Early in the process, the systems

***Statements*** engineer can help identify potential areas where the

Finally, the requirements should be defined in accept- system can be used to collect unique information

able “shall” statements, which are complete sentences that is not directly related to the primary mission.

with a single “shall” per statement. Rationale for the Often outside groups are not aware of the system

requirement should also be captured to ensure the goals and capabilities until it is almost too late in

reason and context of the requirement is understood. the process.

The Key Driving Requirements (KDRs) should be identified. These are requirements that can have a large impact on cost or schedule when implemented. Technical requirements come from a number of

A KDR can have any priority or criticality. Knowing sources including functional, performance, interface,

the impact that a KDR has on the design allows bet- environmental, safety, human interfaces, standards

ter management of requirements. and in support of the “’ilities” such as reliability, sus- tainability, producibility and others. Consideration

See *Appendix C* for guidance and a checklist on how and inclusion of all types of requirements is needed

to write good requirements and *Appendix E* for val- in order to form a complete and consistent set of

idating requirements. A well-written requirements

57

4.0 System Design Processes

NASA SYSTEMS ENGINEERING HANDBOOK

Mission Authority

Mission Objectives

Requirements

Mission Programmatics:

• Cost

• Schedule

• Constraints Customer

• Mission Classification

Implementing Organizations

Requirements Functional System Environmental and Other Design Requirements and Guidelines

Subsystem A Functional and Performance Requirements

Allocated Requirements

FIGURE 4.2-3 The Flowdown of Requirements

It is useful to capture information about each of the requirements, called metadata, for future reference and use. Many requirements management tools will

Institutional Constraints

Assumptions

System Performance Requirements

Subsystem

Subsystem

Subsystem X B

C

Functional and Performance Requirements

Derived Requirements

...

Allocated Requirements

Derived Requirements

document provides several specific benefits to both

request or have options for storing this type of infor- the stakeholders and the technical team as shown in

mation. TABLE 4.2-2 provides examples of the types of TABLE 4.2-1.

metadata that might be useful.

4.2.1.2.4 ***Validate Technical Requirements*** An important part of requirements definition is the validation of the requirements against the stakeholder

58

4.0 System Design Processes

TABLE 4.2-1 Benefits of Well-Written Requirements

Benefit Rationale

Establish the basis for

The complete description of the functions to be performed by the product specified in agreement between the

the requirements will assist the potential users in determining if the product specified stakeholders and the

meets their needs or how the product should be modified to meet their needs. During developers on what the

system design, requirements are allocated to subsystems (e.g., hardware, software, product is to do

and other major components of the system), people, or processes.

Reduce the development effort because less rework is required to address poorly written, missing, and misunderstood requirements

NASA SYSTEMS ENGINEERING HANDBOOK

The Technical Requirements Definition Process activities force the relevant stakeholders to rigorously consider all of the requirements before design begins. Careful review of the requirements can reveal omissions, misunderstandings, and inconsistencies early in the development cycle when these problems are easier to correct thereby reducing costly redesign, remanufacture, recoding, and retesting in later life cycle phases.

Provide a basis for estimating costs and schedules

The description of the product to be developed as given in the requirements is a realistic basis for estimating project costs and can be used to evaluate bids or price estimates.

Provide a baseline for verification and validation

Organizations can develop their verification and validation plans much more productively from a good requirements document. Both system and subsystem test plans and procedures are generated from the requirements. As part of the development, the requirements document provides a baseline against which compliance can be measured. The requirements are also used to provide the stakeholders with a basis for acceptance of the system.

Facilitate transfer The requirements make it easier to transfer the product. Stakeholders thus find it

easier to transfer the product to other parts of their organization, and developers find it easier to transfer it to new stakeholders or reuse it.

Serve as a basis for enhancement

The requirements serve as a basis for later enhancement or alteration of the finished product.

TABLE 4.2-2 Requirements Metadata

Item Function

Requirement ID Provides a unique numbering system for sorting and tracking.

Rationale Provides additional information to help clarify the intent of the requirements at the time they

were written. (See “Rationale” box below on what should be captured.)

Traced from Captures the bidirectional traceability between parent requirements and lower level (derived)

requirements and the relationships between requirements.

Owner Person or group responsible for writing, managing, and/or approving changes to this

requirement.

Verification method Captures the method of verification (test, inspection, analysis, demonstration) and should be

determined as the requirements are developed.

Verification lead Person or group assigned responsibility for verifying the requirement.

Verification level Specifies the level in the hierarchy at which the requirements will be verified (e.g., system,

subsystem, element).

59

4.0 System Design Processes

RATIONALE

The rationale should be kept up to date and include the following information:

• Reason for the Requirement: Often the reason for the requirement is not obvious, and it may be lost if not recorded as the requirement is being documented. The reason may point to a constraint or concept of operations. If there is a clear parent requirement or trade study that explains the reason, then it should be referenced.

• Document Assumptions: If a requirement was written assuming the completion of a technology development program or a successful technology mission, the assumption should be documented.

• Document Relationships: The relationships with the product’s expected operations (e.g., expectations about how stakeholders will use a product) should be documented. This may be done with a link to the ConOps.

• Document Design Constraints: Constraints imposed by the results from decisions made as the design evolves should be documented. If the requirement states a method of implementation, the rationale should state why the decision was made to limit the solution to this one method of implementation.

expectations, the mission objectives and constraints, the concept of operations, and the mission success criteria. Validating requirements can be broken into six steps:

1. Are the Requirements Written Correctly? Identify and correct requirements “shall” state- ment format errors and editorial errors.

2. Are the Requirements Technically Correct? A few trained reviewers from the technical team identify and remove as many technical errors as possible before having all the relevant stakehold- ers review the requirements. The reviewers should check that the requirement statements (a) have bidirectional traceability to the baselined stake- holder expectations; (b) were formed using valid assumptions; and (c) are essential to and consis- tent with designing and realizing the appropriate product solution form that will satisfy the appli- cable product life cycle phase success criteria.

NASA SYSTEMS ENGINEERING HANDBOOK

3. Do the Requirements Satisfy Stakeholders? All relevant stakeholder groups identify and remove defects.

4. Are the Requirements Feasible? All require- ments should make technical sense and be possi- ble to achieve.

5. Are the Requirements Verifiable? All require- ments should be stated in a fashion and with enough information that it will be possible to verify the requirement after the end product is implemented.

6. Are the Requirements Redundant or Over- specified? All requirements should be unique (not redundant to other requirements) and nec- essary to meet the required functions, perfor- mance, or behaviors.

60

4.0 System Design Processes

Requirements validation results are often a decid- ing factor in whether to proceed with the next pro- cess of Logical Decomposition or Design Solution Definition. The project team should be prepared to: (1) demonstrate that the project requirements are complete and understandable; (2) demonstrate that evaluation criteria are consistent with requirements and the operations and logistics concepts; (3) con- firm that requirements and MOEs are consistent with stakeholder needs; (4) demonstrate that oper- ations and architecture concepts support mission needs, goals, objectives, assumptions, guidelines, and constraints; and (5) demonstrate that the process for managing change in requirements is established, doc- umented in the project information repository, and communicated to stakeholders.

4.2.1.2.5 ***Define MOPs and TPMs*** Measures of Performance (MOPs) define the perfor- mance characteristics that the system should exhibit when fielded and operated in its intended environment. MOPs are derived from the MOEs but are stated in more technical terms from the supplier’s point of view. Typically, multiple MOPs, which are quantitative and measurable, are needed to satisfy a MOE, which can be qualitative. From a verification and acceptance point of view, MOPs reflect the system characteristics deemed necessary to achieve the MOEs.

Technical Performance Measures (TPMs) are phys- ical or functional characteristics of the system asso- ciated with or established from the MOPs that are deemed critical or key to mission success. The TPMs are monitored during implementation by comparing the current actual achievement or best estimate of the parameters with the values that were anticipated for the current time and projected for future dates. They are used to confirm progress and identify deficien- cies that might jeopardize meeting a critical system requirement or put the project at cost or schedule risk.

NASA SYSTEMS ENGINEERING HANDBOOK

For additional information on MOPs and TPMs, their relationship to each other and MOEs, and examples of each, see Section 6.7.2.6.2 of the NASA Expanded Guidance for SE document at *https://nen. nasa.gov/web/se/doc-repository*.

4.2.1.2.6 ***Establish Technical Requirement Baseline*** Once the technical requirements are identified and validated to be good (clear, correct, complete, and achievable) requirements, and agreement has been gained by the customer and key stakeholders, they are baselined and placed under configuration control. Typically, a System Requirements Review (SRR) is held to allow comments on any needed changes and to gain agreement on the set of requirements so that it may be subsequently baselined. For additional infor- mation on the SRR, see *Section 6.7*.

4.2.1.2.7 ***Capture Work Products*** The work products generated during the above activ- ities should be captured along with key decisions that were made, any supporting decision rationale and assumptions, and lessons learned in performing these activities.

4.2.1.3 *Outputs*

• Validated Technical Requirements: This is the approved set of requirements that represents a complete description of the problem to be solved and requirements that have been validated and approved by the customer and stakeholders. Examples of documents that capture the require- ments are a System Requirements Document (SRD), Project Requirements Document (PRD), Interface Requirements Document (IRD), and a Software Requirements Specification (SRS).

• Measures of Performance: These are the iden- tified quantitative measures that, when met by the design solution, help ensure that one or more MOEs will be satisfied. There may be

61

4.0 System Design Processes

two or more MOPs for each MOE. See Section 6.7.2.6.2in the NASA Expanded Guidance for Systems Engineering at *https://nen.nasa.gov/web/ se/doc-repository* for further details.

• Technical Performance Measures: These are the set of performance measures that are monitored and trended by comparing the current actual achievement of the parameters with that expected or required at the time. TPMs are used to confirm progress and identify deficiencies. See Section 6.7.2.6.2 in the NASA Expanded Guidance for Systems Engineering at *https://nen.nasa.gov/web/ se/doc-repository* for further details.

4.2.2 Technical Requirements

Definition Guidance Refer to Section 4.2.2 of the NASA Expanded Guidance for SE document at *https://nen.nasa.gov/ web/se/doc-repository* for additional information on:

• types of requirements,

• requirements databases, and

• the use of technical standards.

4.3 Logical Decomposition

Logical decomposition is the process for creating the detailed functional requirements that enable NASA programs and projects to meet the stakeholder expec- tations. This process identifies the “what” that should be achieved by the system at each level to enable a successful project. Logical decomposition utilizes functional analysis to create a system architecture and to decompose top-level (or parent) requirements and allocate them down to the lowest desired levels of the project.

The Logical Decomposition Process is used to:

• Improve understanding of the defined techni- cal requirements and the relationships among

NASA SYSTEMS ENGINEERING HANDBOOK

the requirements (e.g., functional, performance, behavioral, and temporal etc.), and

• Decompose the parent requirements into a set of logical decomposition models and their associated sets of derived technical requirements for input to the Design Solution Definition Process.

4.3.1 Process Description FIGURE 4.3-1 provides a typical flow diagram for the Logical Decomposition Process and identifies typical inputs, outputs, and activities to consider in address- ing logical decomposition.

4.3.1.1 *Inputs* Typical inputs needed for the Logical Decomposition Process include the following:

• Technical Requirements: A validated set of requirements that represent a description of the problem to be solved, have been established by functional and performance analysis, and have been approved by the customer and other stake- holders. Examples of documents that capture the requirements are an SRD, PRD, and IRD.

• Technical Measures: An established set of mea- sures based on the expectations and requirements that will be tracked and assessed to determine overall system or product effectiveness and cus- tomer satisfaction. These measures are MOEs, MOPs, and a special subset of these called TPMs. See Section 6.7.2.6.2 in the NASA Expanded Guidance for Systems Engineering at *https://nen. nasa.gov/web/se/doc-repository* for further details.

4.3.1.2 *Process Activities* 4.3.1.2.1 ***Define One or More Logical Decomposition***

***Models*** The key first step in the Logical Decomposition Process is establishing the system architecture model. The system architecture activity defines the

62

4.0 System Design Processes

*From* **Technical Requirements Definition**

Define one or more logical decomposition models

NASA SYSTEMS ENGINEERING HANDBOOK

*To* **Design Solution and Requirements** and **Interface Management Processes** and **Configuration Managemen**

**t Processes**

Allocate technical requirements to Baselined Technical

logical decomposition models to form

Derived Technical Requirements

Requirements

a set of derived technical requirements

Resolve derived technical **Requirements Definition**

requirements conflicts

Logical Decomposition Models

Measures of Performance

Validate the resulting set of derived technical requirements

*To* **Technical Data Management Process**

Establish the derived technical

Logical Decomposition requirements baseline

Work Products

Capture work products from logical decomposition activities

FIGURE 4.3-1 Logical Decomposition Process

Once the top-level (or parent) functional require- ments and constraints have been established, the system designer uses functional analysis to begin to formulate a conceptual system architecture. The system architecture can be seen as the strategic orga- nization of the functional elements of the system, laid out to enable the roles, relationships, dependen- cies, and interfaces between elements to be clearly

*To* **Design Solution** and **Configuration** *From* **Technical**

**Management Processes**

and **Technical Data Management Processes**

underlying structure and relationships of hardware, software, humans-in-the-loop, support personnel, communications, operations, etc., that provide for the implementation of Agency, mission director- ate, program, project, and subsequent levels of the requirements. System architecture activities drive the partitioning of system elements and requirements to lower level functions and requirements to the point that design work can be accomplished. Interfaces and relationships between partitioned subsystems and elements are defined as well.

defined and understood. It is strategic in its focus on the overarching structure of the system and how its elements fit together to contribute to the whole, instead of on the particular workings of the elements themselves. It enables the elements to be developed separately from each other while ensuring that they work together effectively to achieve the top-level (or parent) requirements.

Much like the other elements of functional decom- position, the development of a good system-level architecture is a creative, recursive, collaborative, and iterative process that combines an excellent under- standing of the project’s end objectives and constraints with an equally good knowledge of various potential technical means of delivering the end products.

Focusing on the project’s ends, top-level (or parent) requirements, and constraints, the system architect should develop at least one, but preferably multiple,

63

4.0 System Design Processes

concept architectures capable of achieving program objectives. Each architecture concept involves spec- ification of the functional elements (what the pieces do), their relationships to each other (interface defi- nition), and the ConOps, i.e., how the various seg- ments, subsystems, elements, personnel, units, etc., will operate as a system when distributed by location and environment from the start of operations to the end of the mission.

The development process for the architectural con- cepts should be recursive and iterative with feedback from stakeholders and external reviewers, as well as from subsystem designers and operators, provided as often as possible to increase the likelihood of effec- tively achieving the program’s desired ends while reducing the likelihood of cost and schedule overruns.

In the early stages of development, multiple con- cepts are generated. Cost and schedule constraints will ultimately limit how long a program or project can maintain multiple architectural concepts. For all NASA programs, architecture design is completed during the Formulation Phase. For most NASA proj- ects (and tightly coupled programs), the baselining of a single architecture happens during Phase A. Architectural changes at higher levels occasionally occur as decomposition to lower levels produces com- plexity in design, cost, or schedule that necessitates such changes. However, as noted in FIGURE 2.5-1, the later in the development process that changes occur, the more expensive they become.

Aside from the creative minds of the architects, there are multiple tools that can be utilized to develop a system’s architecture. These are primarily modeling and simulation tools, functional analysis tools, archi- tecture frameworks, and trade studies. (For example, one way of doing architecture is the Department of Defense (DOD) Architecture Framework (DODAF). A search concept is developed, and analytical models of the architecture, its elements, and their operations

NASA SYSTEMS ENGINEERING HANDBOOK

are developed with increased fidelity as the project evolves. Functional decomposition, requirements development, and trade studies are subsequently undertaken. Multiple iterations of these activities feed back to the evolving architectural concept as the requirements flow down and the design matures.

4.3.1.2.2 ***Allocate Technical Requirements, Resolve***

***Conflicts, and Baseline*** Functional analysis is the primary method used in system architecture development and functional requirement decomposition. It is the systematic pro- cess of identifying, describing, and relating the func- tions a system should perform to fulfill its goals and objectives. Functional analysis identifies and links system functions, trade studies, interface character- istics, and rationales to requirements. It is usually based on the ConOps for the system of interest.

Three key steps in performing functional analysis are:

1. Translate top-level requirements into functions that should be performed to accomplish the requirements.

2. Decompose and allocate the functions to lower

levels of the product breakdown structure.

3. Identify and describe functional and subsystem

interfaces.

The process involves analyzing each system require- ment to identify all of the functions that need to be performed to meet the requirement. Each function identified is described in terms of inputs, outputs, failure modes, consequence of failure, and inter- face requirements. The process is repeated from the top down so that sub-functions are recognized as part of larger functional areas. Functions are arranged in a logical sequence so that any specified operational usage of the system can be traced in an end-to-end path.

64

4.0 System Design Processes

The process is recursive and iterative and continues until all desired levels of the architecture/system have been analyzed, defined, and baselined. There will almost certainly be alternative ways to decompose functions. For example, there may be several ways to communicate with the crew: Radio Frequency (RF), laser, Internet, etc. Therefore, the outcome is highly dependent on the creativity, skills, and experience of the engineers doing the analysis. As the analysis proceeds to lower levels of the architecture and sys- tem, and the system is better understood, the systems engineer should keep an open mind and a willingness to go back and change previously established archi- tecture and system requirements. These changes will then have to be decomposed down through the archi- tecture and sub-functions again with the recursive process continuing until the system is fully defined with all of the requirements understood and known to be viable, verifiable, and internally consistent. Only at that point should the system architecture and requirements be baselined.

4.3.1.2.3 ***Capture Work Products*** The other work products generated during the Logical Decomposition Process should be captured along with key decisions made, supporting decision rationale and assumptions, and lessons learned in performing the activities.

4.3.1.3 *Outputs* Typical outputs of the Logical Decomposition Process include the following:

• Logical Decomposition Models: These models define the relationship of the requirements and functions and their behaviors. They include the system architecture models that define the under- lying structure and relationship of the elements of the system (e.g., hardware, software, humans- in-the-loop, support personnel, communications, operations, etc.) and the basis for the partitioning

NASA SYSTEMS ENGINEERING HANDBOOK

of requirements into lower levels to the point that design work can be accomplished.

• Derived Technical Requirements: These are requirements that arise from the definitions of the selected architecture that were not explicitly stated in the baselined requirements that served as an input to this process. Both the baselined and derived requirements are allocated to the system architecture and functions.

• Logical Decomposition Work Products: These are the other products generated by the activities of this process.

4.3.2 Logical Decomposition

Guidance Refer to Section 4.3.2 and Appendix F in the NASA Expanded Guidance for Systems Engineering at *https://nen.nasa.gov/web/se/doc-repository* for addi- tional guidance on:

• Product Breakdown Structures and

• Functional Analysis Techniques.

4.4 Design Solution Definition

The Design Solution Definition Process is used to translate the high-level requirements derived from the stakeholder expectations and the outputs of the Logical Decomposition Process into a design solu- tion. This involves transforming the defined logical decomposition models and their associated sets of derived technical requirements into alternative solu- tions. These alternative solutions are then analyzed through detailed trade studies that result in the selection of a preferred alternative. This preferred alternative is then fully defined into a final design solution that satisfies the technical requirements. This design solution definition is used to generate the end product specifications that are used to produce

65

4.0 System Design Processes

the product and to conduct product verification. This

• Technical Requirements: These are the customer process may be further refined depending on whether

and stakeholder needs that have been translated there are additional subsystems of the end product

into a complete set of validated requirements for that need to be defined.

the system, including all interface requirements.

4.4.1 Process Description

• Logical Decomposition Models: Requirements FIGURE 4.4-1 provides a typical flow diagram for the

are analyzed and decomposed by one or more Design Solution Definition Process and identifies

different methods (e.g., function, time, behavior, typical inputs, outputs, and activities to consider in

data flow, states, modes, system architecture, etc.) addressing design solution definition.

in order to gain a more comprehensive under- standing of their interaction and behaviors. (See 4.4.1.1 *Inputs*

the definition of a model in *Appendix B*.) There are several fundamental inputs needed to initi- ate the Design Solution Definition Process:

*\* To* **Implementation Process**

NASA SYSTEMS ENGINEERING HANDBOOK

*To* **Requirements** and **Interface Management Processes**

System-Speci d

Define alternative design solutions

Requirements

Analyze each alternative design solution

Select best design solution alternative

Initial Su Generate full design description of the

Specifications selected solution

Verify

Capture work products from design solution definition activities

End Product–Specified Requirements

*From* **Logical Decomposition** and **Configuration Management**

*To* **Stakeholder Expectations Definition** and **Requirements** and **Interface Management Processes Processes**

Product Verification Plan

Product Validation Plan

Initiate development of enabling products

bsystem Baselined Logical Decomposition Models

*To* **Stakeholder Expectations Definition** or **Product Implementation** and the fully defined design solution

**Requirements** and **Interface Management Processes** Baselined Derived Technical Requirements

Baseline design solution specified requirements and design descriptions

No

\*

FIGURE 4.4-1 Design Solution Definition Process

Enabling Product Requirements

*To* **Product Verification Process**

Yes

Enabling \*

product exists?

Need lower level product?

*To* **Product Validation Process**

No Yes

Initiate development of next lower level

*To* **Technical Data Management Process** products

Logistics and Operate- To Procedures

66

4.0 System Design Processes

4.4.1.2 *Process Activities* 4.4.1.2.1 ***Define Alternative Design Solutions*** The realization of a system over its life cycle involves a succession of decisions among alternative courses of action. If the alternatives are precisely defined and thoroughly understood to be well differentiated in the cost-effectiveness space, then the systems engi- neer can make choices among them with confidence.

To obtain assessments that are crisp enough to facili- tate good decisions, it is often necessary to delve more deeply into the space of possible designs than has yet been done, as illustrated in FIGURE 4.4-2. It should be realized, however, that this illustration represents neither the project life cycle, which encompasses the system development process from inception through disposal, nor the product development pro- cess by which the system design is developed and implemented.

NASA SYSTEMS ENGINEERING HANDBOOK

Increasreesolution

Increasreesolution

FIGURE 4.4-2 The Doctrine of Successive Refinement

Each “create concepts” step in FIGURE 4.4-2 involves a recursive and iterative design loop driven by the set of stakeholder expectations where a straw man architec- ture/design, the associated ConOps, and the derived requirements are developed and programmatic con- straints such as cost and schedule are considered. These three products should be consistent with each other and will require iterations and design decisions to achieve this consistency. This recursive and itera- tive design loop is illustrated in FIGURE 4.0-1.

Each “create concepts” step in FIGURE 4.4-2 also involves an assessment of potential capabilities offered by the continually changing state of technology and potential pitfalls captured through experience-based review of prior program/project lessons learned data. It is imperative that there be a continual interaction between the technology development process, cross- cutting processes such as human systems integration, and the design process to ensure that the design reflects the realities of the available technology and that overreliance on immature technology is avoided.

Recognize need/ opportunity

Identify and quantify goals

Identify and quantify goals

Identify and quantify goals

Identify and quantify goalsconcepts

cCreate Increasreesolution

concepts

concepts Create

Create

Additionally, the state of any technology that is con- sidered enabling should be properly monitored, and care should be taken when assessing the impact of this technology on the concept performance. This interaction is facilitated through a periodic assess- ment of the design with respect to the maturity of the technology required to implement the design. (See Section 4.4.2.1 in the NASA Expanded Guidance for Systems Engineering at *https://nen.nasa.gov/web/ se/doc-repository* for a more detailed discussion of technology assessment.) These technology elements usually exist at a lower level in the PBS. Although the process of design concept development by the integration of lower level elements is a part of the systems engineering process, there is always a danger that the top-down process cannot keep up with the bottom-up process. Therefore, system architecture issues need to be resolved early so that the system can be modeled with sufficient realism to do reliable trade studies.

As the system is realized, its particulars become clearer—but also harder to change. See the rising

oncepts

**Implement decisions**

Do sttruadde ieDo Perform s sttruaDddo e iests truadde

ies mission Create

desigSelen

ct Do sttruaddiee s

desigSelen ct desigSelect n desigSelect n

67

4.0 System Design Processes

“Cost to Change Design Direction” in FIGURE 2.5-1. The purpose of systems engineering is to make sure that the Design Solution Definition Process happens in a way that leads to the most functional, safe, and cost-effective final system while working within any given schedule boundaries. The basic idea is that before those decisions that are hard to undo are made, the alternatives should be carefully and itera- tively assessed, particularly with respect both to the maturity of the required technology and to stake- holder expectations for efficient, effective operations.

4.4.1.2.2 ***Create Alternative Design Concepts*** Once it is understood what the system is to accom- plish, it is possible to devise a variety of ways that those goals can be met. Sometimes, that comes about as a consequence of considering alternative func- tional allocations and integrating available subsystem design options, all of which can have technologies at varying degrees of maturity. Ideally, as wide a range of plausible alternatives as is consistent with the design organization’s charter should be defined, keeping in mind the current stage in the process of successive refinement. When the bottom-up process is operat- ing, a problem for the systems engineer is that the designers tend to become fond of the designs they create, so they lose their objectivity; the systems engi- neer should stay an “outsider” so that there is more objectivity. This is particularly true in the assessment of the technological maturity of the subsystems and components required for implementation. There is a tendency on the part of technology developers and project management to overestimate the maturity and applicability of a technology that is required to implement a design. This is especially true of “heri- tage” equipment. The result is that critical aspects of systems engineering are often overlooked.

The creation of alternative design solutions involves assessment of potential capabilities offered by the continually changing state of technology. A continual

NASA SYSTEMS ENGINEERING HANDBOOK

interaction between the technology development process and the design process ensures that the design reflects the realities of the available technology. This interaction is facilitated through periodic assessment of the design with respect to the maturity of the tech- nology required to implement the design.

After identifying the technology gaps existing in a given design concept, it is frequently necessary to undertake technology development in order to ascertain viability. Given that resources will always be limited, it is necessary to pursue only the most promising technologies that are required to enable a given concept.

If requirements are defined without fully under- standing the resources required to accomplish needed technology developments, then the program/project is at risk. Technology assessment should be done iter- atively until requirements and available resources are aligned within an acceptable risk posture. Technology development plays a far greater role in the life cycle of a program/project than has been traditionally con- sidered, and it is the role of the systems engineer to develop an understanding of the extent of program/ project impacts—maximizing benefits and minimiz- ing adverse effects. Traditionally, from a program/ project perspective, technology development has been associated with the development and incorpo- ration of any “new” technology necessary to meet requirements. However, a frequently overlooked area is that associated with the modification of “heritage” systems incorporated into different architectures and operating in different environments from the ones for which they were designed. If the required modifica- tions and/or operating environments fall outside the realm of experience, then these too should be consid- ered technology development.

To understand whether or not technology develop- ment is required—and to subsequently quantify the

68

4.0 System Design Processes

associated cost, schedule, and risk—it is necessary to systematically assess the maturity of each system, subsystem, or component in terms of the architecture and operational environment. It is then necessary to assess what is required in the way of development to advance the maturity to a point where it can success- fully be incorporated within cost, schedule, and per- formance constraints. A process for accomplishing this assessment is described in *Appendix G*. Because technology development has the potential for such significant impacts on a program/project, technology assessment needs to play a role throughout the design and development process from concept development through Preliminary Design Review (PDR). Lessons learned from a technology development point of view should then be captured in the final phase of the program.

On the first turn of the successive refinement in FIGURE 4.4-2, the subject is often general approaches or strategies, sometimes architectural concepts. On the next, it is likely to be functional design, then detailed design, and so on. The reason for avoiding a premature focus on a single design is to permit dis- covery of the truly best design. Part of the systems engineer’s job is to ensure that the design concepts to be compared take into account all interface require- ments. Characteristic questions include: “Did you include the cabling?” or “Did you consider how the maintainers can repair the system?” When possible, each design concept should be described in terms of controllable design parameters so that each rep- resents as wide a class of designs as is reasonable. In doing so, the systems engineer should keep in mind that the potentials for change may include organi- zational structure, personnel constraints, schedules, procedures, and any of the other things that make up a system. When possible, constraints should also be described by parameters.

NASA SYSTEMS ENGINEERING HANDBOOK

4.4.1.2.3 ***Analyze Each Alternative Design Solution*** The technical team analyzes how well each of the design alternatives meets the system objectives (tech- nology gaps, effectiveness, technical achievability, performance, cost, schedule, and risk, both quanti- fied and otherwise). This assessment is accomplished through the use of trade studies. The purpose of the trade study process is to ensure that the system archi- tecture, intended operations (i.e., the ConOps) and design decisions move toward the best solution that can be achieved with the available resources. The basic steps in that process are:

• Devise some alternative means to meet the func- tional requirements. In the early phases of the project life cycle, this means focusing on system architectures; in later phases, emphasis is given to system designs.

• Evaluate these alternatives in terms of the MOPs and system life cycle cost. Mathematical models are useful in this step not only for forcing rec- ognition of the relationships among the outcome variables, but also for helping to determine what the MOPs should be quantitatively.

• Rank the alternatives according to appropriate selection criteria.

• Drop less promising alternatives and proceed to the next level of resolution, if needed.

The trade study process should be done openly and inclusively. While quantitative techniques and rules are used, subjectivity also plays a significant role. To make the process work effectively, participants should have open minds, and individuals with dif- ferent skills—systems engineers, design engineers, crosscutting specialty discipline and domain engi- neers, program analysts, system end users, deci- sion scientists, maintainers, operators, and project

69

4.0 System Design Processes

managers—should cooperate. The right quantita- tive methods and selection criteria should be used. Trade study assumptions, models, and results should be documented as part of the project archives. The participants should remain focused on the functional requirements, including those for enabling products. For an in-depth discussion of the trade study process, see *Section 6.8*. The ability to perform these studies is enhanced by the development of system models that relate the design parameters to those assessments, but it does not depend upon them.

The technical team should consider a broad range of concepts when developing the system model. The model should define the roles of crew, operators, maintainers, logistics, hardware, and software in the system. It should identify the critical technolo- gies required to implement the mission and should consider the entire life cycle from fabrication to disposal. Evaluation criteria for selecting concepts should be established. Cost is always a limiting fac- tor. However, other criteria, such as time to develop and certify a unit, risk, and reliability, also are crit- ical. This stage cannot be accomplished without addressing the roles of operators and maintainers. These contribute significantly to life cycle costs and to the system reliability. Reliability analysis should be performed based upon estimates of component fail- ure rates for hardware and an understanding of the consequences of these failures. If probabilistic risk assessment models are applied, it may be necessary to include occurrence rates or probabilities for software faults or human error events. These models should include hazard analyses and controls implemented through fault management. Assessments of the matu- rity of the required technology should be done and a technology development plan developed.

Controlled modification and development of design concepts, together with such system models, often permits the use of formal optimization techniques

NASA SYSTEMS ENGINEERING HANDBOOK

to find regions of the design space that warrant fur- ther investigation.

Whether system models are used or not, the design concepts are developed, modified, reassessed, and compared against competing alternatives in a closed- loop process that seeks the best choices for further development. System and subsystem sizes are often determined during the trade studies. The end result is the determination of bounds on the relative cost-ef- fectiveness of the design alternatives, measured in terms of the quantified system goals. (Only bounds, rather than final values, are possible because deter- mination of the final details of the design is inten- tionally deferred.) Increasing detail associated with the continually improving resolution reduces the spread between upper and lower bounds as the pro- cess proceeds.

4.4.1.2.4 ***Select the Best Design Solution Alternative*** The technical team selects the best design solution from among the alternative design concepts, taking into account subjective factors that the team was unable to quantify, such as robustness, as well as estimates of how well the alternatives meet the quan- titative requirements; the maturity of the available technology; and any effectiveness, cost, schedule, risk, or other constraints.

The Decision Analysis Process, as described in *Section 6.8*, should be used to make an evaluation of the alternative design concepts and to recommend the “best” design solution.

When it is possible, it is usually well worth the trou- ble to develop a mathematical expression, called an “objective function,” that expresses the values of com- binations of possible outcomes as a single measure of cost-effectiveness, as illustrated in FIGURE 4.4-3, even if both cost and effectiveness should be described by more than one measure.

70