Federal Aviation Administration

FAA Systems Engineering Manual

Version 1.0.1
June 19, 2014

TC13-0041

This page intentionally left blank.

FAA Systems Engineering Manual

Version 1.0

Approved by: Michele Merkle Date: 3-21-14
Michele Merkle, Director of NAS Systems Engineering Services, ANG-B

Approved by: Date: 3-21-14
Steven Bradford, Technical Review Board chair

Focal Point

Kimberly Gill
ANG-B1
202-385-7214

Federal Aviation Administration
800 Independence Avenue SW
Washington, DC 20591

Document Revision History

Version	***Date***	***Description of Change***	***Person***
1.0	*3/21/14*	*Initial release of the FAA Systems Engineering Manual. Approved by the TRB*	*SEM Team*
1.0.1	*6/19/14*	*Additional changes per ASAG and ARB request*	*L. Marsh*

Table of Contents

Table of Figures

Table of Tables

Preface

Federal Aviation Administration (FAA) Systems Engineering Manual (SEM) Version 1.0 describes the framework for implementing essential systems engineering practices across the agency. The SEM defines the systems engineering practices that FAA employees should follow, and specifies how the agency agrees to implement these practices in order to accomplish the mission of providing the safest, most efficient aerospace system in the world.

The previous SEM – the National Airspace System SEM, Version 3.1 – was published in 2006. In the intervening years many users of the document have expressed suggestions for improving usability and adding important content. In 2012, a number of workshops were convened to solicit further recommendations. Because systems engineering is a constantly evolving discipline with continual new developments, the FAA appointed a team to revise the SEM based on current government and industry best practices and standards. The SEM team reviewed systems engineering manuals within federal and state governments, as well as industry, to determine an acceptable approach for an FAA-wide systems engineering manual.

Version 1.0 of the FAA SEM also includes recommendations from a September 2008 report entitled "*Identifying the Workforce to Respond to a National Imperative – The Next Generation Air Transportation System".* The Next Generation Air Transportation System (NextGen) is a comprehensive overhaul of the National Airspace System (NAS) to make air travel more efficient and dependable, while ensuring each flight is as safe and secure as possible. In order to complete the transformation to NextGen and continue supporting the nation's air transportation system, it is essential that FAA follow systems engineering best practices. Additionally, the National Academy of Public Administration called for the improvement of systems engineering competencies within the FAA while supporting the transition to NextGen.

The development team for FAA SEM Version 1.0 owes a debt of gratitude to the many authors, editors and reviewers who contributed to this document and the versions that preceded it. We endeavored to address the vast majority of the recommendations and balanced conflicting approaches to topics.

After the publication of SEM Version 1.0, an update is scheduled to occur every 1-2 years. The goal is to incorporate and update links to policy, guidance, and example documentation and to otherwise continually improve the usefulness of the SEM for its intended audience. To submit feedback on the SEM, please send e-mail to *SEforum@faa.gov.*

This page intentionally left blank.

1 Introduction

The Federal Aviation Administration (FAA) Systems Engineering Manual (SEM) is a guidance document, which defines major systems engineering (SE) elements combined with industry and government best practices to be implemented in the context of FAA operations.

Systems engineering is a discipline that concentrates on the design and application of the whole system as distinct from its parts. At the Enterprise level, systems engineering management integrates across investment programs to achieve an efficient and highly interoperable FAA. At the program level, it optimizes performance, benefits, operations, and lifecycle costs. Individual programs tailor the application of processes, tools, and techniques, according to the complexity of the program's requirements. The SEM is a compilation of industry- and government-proven practices within the SE domain that are deemed applicable to support the agency's business needs.

SE best practices defined in this SEM should be applied to manage complexity and change in the FAA while achieving the defined mission and meeting the associated needs. To maximize effectiveness, SE commences when the need is identified and continues throughout the program's lifecycle. *When performed correctly, SE helps to ensure that program execution follows best practices*. SE helps to ensure that deficiencies are detected and resolved early in the acquisition lifecycle, resulting in reduced risk and fewer cost and schedule overruns.

1.1 Purpose and Scope

The purpose of this manual is to provide a framework for implementing systems engineering across the FAA. This SEM supports the FAA's shift towards NextGen by providing the following guidance:

1. Defines FAA's preferred SE processes to be used by any engineer or group performing a task requiring an SE approach.
2. Must be followed throughout the Acquisition Management System (AMS) lifecycle
3. Provides effective SE methods and tools
4. Identifies competency areas for the effective practice of SE

The SEM supports the AMS life cycle phases by identifying the proper application of SE elements in the AMS decision and acquisition processes. This manual defines System Engineering best practices used to support Program Management activities. The SEM also acts as a reference for the development of training classes within the FAA.

1.2 Audience

The SEM provides guidance for any FAA employee who needs information on performing SE processes and developing solutions to SE issues facing the agency. The document is written for a broad audience of practitioners: new FAA systems engineers, program managers, an engineer in another discipline who needs to perform systems engineering, those in specialty engineering (e.g., Human Systems Integration), and the experienced systems engineer who needs a convenient reference for implementing SE practices within the FAA context. Table 1 shows how some primary users benefit from the SEM.

Table 1: User Roles and Uses of SEM

User Role	Use of SEM		
	Training (as needed)	Reference	Primary Business Use
Program Manager		X	Provides an understanding of Systems Engineering (SE) tasks performed by team members.
Junior Systems Engineer	X	X	Provides a foundational understanding of how SE is accomplished within the FAA framework
Senior Systems Engineer	X	X	Provides guidance on SE topics with which the user is not current
Other Engineer	X	X	Provides an understanding of what SE work needs to be done and preferred methodology
Subject Matter Expert (SME)	X	X	Provides an understanding of how SME input is incorporated into SE processes
Specialty Engineers	As applicable	X	Provides an understanding of how the specialty engineering work is integrated into SE processes
Test Practioner		X	Provides an understanding of the testing support the SE is expecting from the test community

1.3 Document Overview

The SEM provides the framework for implementing SE within the FAA. The following sections describe the many processes and activities that make up systems engineering throughout the lifecycle of a solution, project, or program:

- Section 2: Systems Engineering and the AMS Lifecycle
- Section 3: Systems Engineering Processes
- Section 4: Technical Management
- Section 5: Specialty Engineering
- Appendices to provide additional details on topics addressed by the previous sections

Section 2: Systems Engineering and the AMS Lifecycle describes the phases that a needed solution goes through from identification of the stakeholder needs to use of the solution in the operational environment. Systems engineering roles, best practices, and products are identified for each AMS phase.

Section 3: Systems Engineering Processes are disciplines which describe how to generate systems engineering products and artifacts (documents). They are undertaken iteratively throughout the systems engineering lifecycle, and perform the following functions:

- Determine and document operational concepts;
- Conduct effective functional analysis;
- Define the requirements for a system;
- Transform the requirements into an effective solution via design specifications;
- Support successful deployment of the solution; and
- Prepare the required systems engineering documentation.

Section 4: Technical Management describes a holistic management approach that promotes process effectiveness and ensures that all planned and systematic activities associated with those processes are of the highest quality. The technical management processes are the overarching mechanisms that enable the systems engineering processes to iterate and achieve more detailed documentation over the AMS lifecycle.

Section 5: Specialty Engineering plays an integral role in a successful engineering effort. The specialty engineering disciplines described in the SEM are Reliability, Maintainability, and Availability (RMA); Lifecycle Engineering; Electromagnetic Environmental Effects and Spectrum Management; Human Factors Engineering; Information Security Engineering; System Safety Engineering; and Hazardous Materials Management and Environmental Engineering.

Figure 1 is a graphical overview of FAA systems engineering. The top row lists the AMS lifecycle phases used by every significant NAS or non-NAS project to track solution development. The brown box contains all of the processes and techniques called upon throughout the lifecycle phases and detailed in the SEM. Generally, the SE processes – in green – adhere to the principles and techniques of Technical Management listed in the purple boxes; Specialty Engineering disciplines are engaged whenever they are needed. SE processes iterate and create successively more detailed solution documentation; the beige box to the right lists the primary examples.

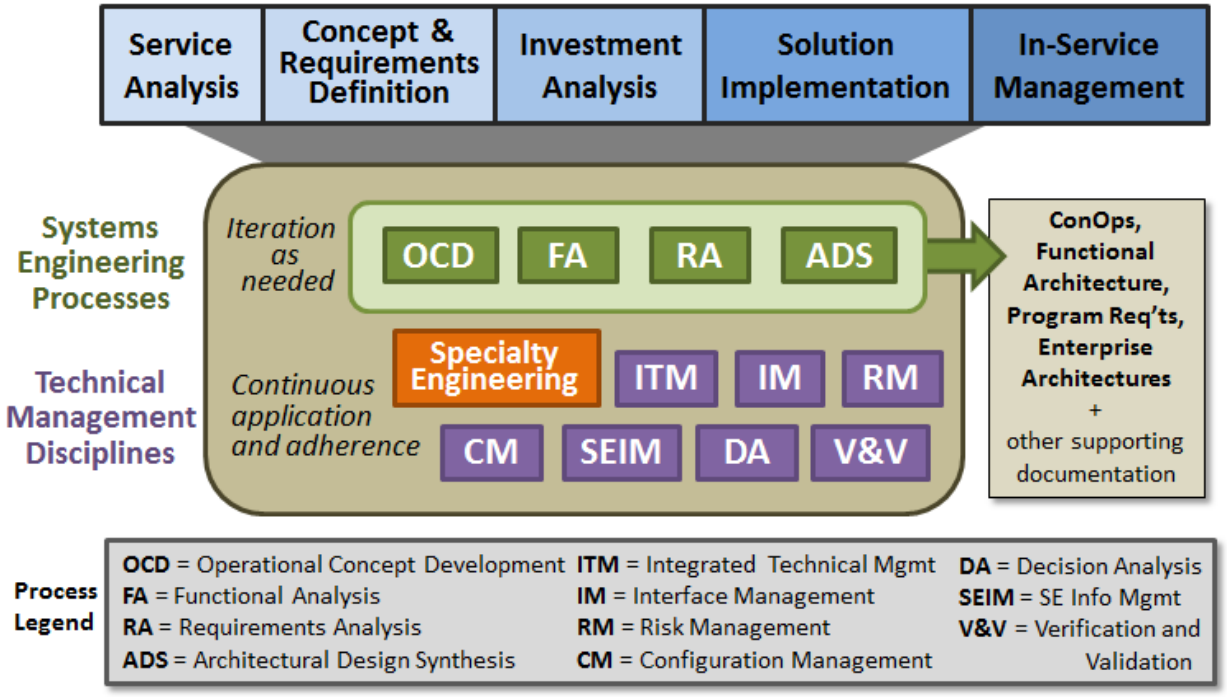


Figure 1: FAA Systems Engineering Overview

1.4 Plan, Do, Check, Act

The Systems Engineering Processes and the Technical Management Processes in this SEM can iterate throughout several phases of the acquisition lifecycle of a project. For some processes, the systems engineer may consider using the Plan, Do, Check, Act (PDCA) cycle to assist in organizing the work and also enable continuous process improvement.

The concept of the PDCA cycle was originally developed by Walter Shewhart, the pioneering statistician who developed statistical process control in the Bell Laboratories in the 1930s. PDCA was made popular

by Dr. W. Edwards Deming who is considered by many to be the father of modern quality control. He always referred to it as the "Shewhart cycle". Later in Deming's career, he modified PDCA to "Plan, Do, Study, Act" because he felt that "check" emphasized inspection over analysis (Anderson 2011). Figure 2 is a graphical depiction of the cycle.

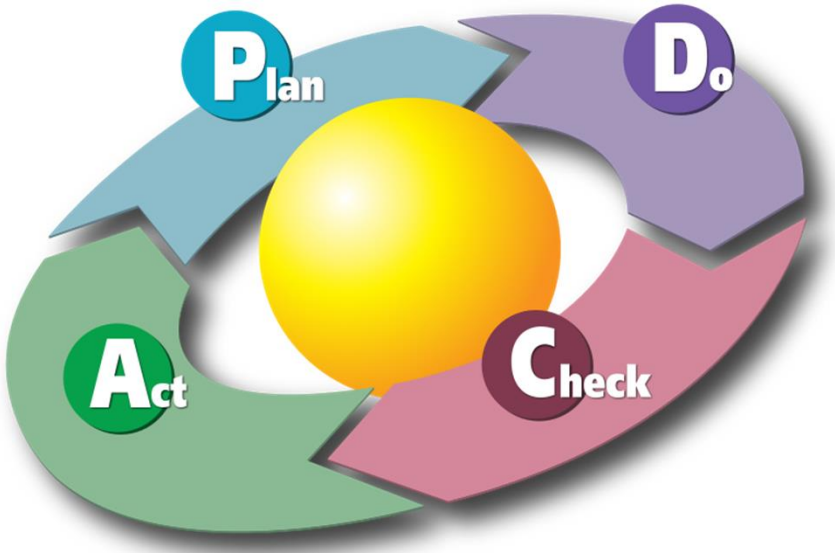


Figure 2: Plan, Do, Check, Act Cycle

The steps in each successive PDCA cycle are:

- **PLAN:** Come up with ideas on how to solve identified problems. Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the delivered product or service can be measured. When possible, start on a small scale to test the results of the processes for adverse or unexpected effects.
- **DO:** Implement the plan, execute the process, make the product or provide the service. Collect data for documenting, diagramming, and analysis in the following "CHECK" and "ACT" steps.
- **CHECK:** Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do". Documenting data can make it much easier to see trends over several PDCA cycles and convert the collected data into information. Information is what you need for the next step "ACT".
- **ACT:** Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product. When a pass through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve with more detail in the next iteration of the cycle, or attention needs to be placed in a different stage of the process.

Note: some modern trainers also refer to the "A" as "Adjust". This helps trainees to understand that the fourth step is more about correcting the difference between the current state and the planned state instead of thinking that the "A" is all about action and implementation (which actually happens in the second ("D") stage).

A basic example of the use of PDCA is shown in Appendix D: Example of Using PDCA.

1.5 System of Systems

As FAA develops the Next Generation Air Transportation System (NextGen), the National Airspace System (NAS) is evolving into a more complex System of Systems (SoS). Even in the non-NAS portion of FAA, SoS are evolving. To address a SoS, the systems engineer needs to know what one is and what unique challenges it brings. SoS is a relatively recent concept with few established SE processes specifically geared toward it. This section introduces definitions, some integration issues that must be overcome, and a list of SEM technical processes where special SoS guidance is included.

A “system” can be defined in numerous ways. The International Council on Systems Engineering (INCOSE) handbook defines a system as “a combination of interacting elements organized to achieve one or more stated purposes." The previous SEM states, “A system is an integrated set of constituent pieces that are combined in an operational or support environment to accomplish a defined objective. These pieces include people, hardware, software, firmware, information, procedures, facilities, services, and other support facets.“ Both definitions are useful when considering a system of systems.

1.5.1 What is a System of Systems?

A SoS is a collection of independent systems that work together to achieve some common purpose. There can also be distinguishing characteristics, such as physically distributed systems, functionality that emerges from the connections between systems, and system heterogeneity (Maier 1998). A SoS can evolve over time and is more complex than developing stand-alone systems. Heterogeneous systems within a SoS are integrated to work effectively together. The union of unique component systems forms a new SoS with a different function than any one of the individual systems has, and the various systems within a SoS can achieve results together that they could not do alone (Carlock 2001).

In a true SoS, each component system must have its own purpose independent of the other systems, and the component systems must maintain their independence. An example of a SoS is Automatic Dependent Surveillance-Broadcast (ADS-B), which provides shared situational awareness to different facilities and aircraft in the NAS. It obtains information from the Global Positioning System (GPS), broadcasts this information using aircraft transponders, is received by other aircraft using similar transponders, is received by radio stations on the ground and distributed by a communications network to ATC facilities, and is processed and displayed by ATC automation systems such as Standard Terminal Automation Replacement System (STARS) and En Route Automation Modernization (ERAM). These systems operate independently, but in their combination provide ADS-B capabilities in the NAS.

Advantages of System of Systems

A SoS has emergent capabilities and properties that do not reside in the component systems. By its nature, SoS provides better interoperability among the component systems. The importance lies in recognizing a SoS as such and the unique challenges presented to the systems engineer. System interdependencies and relationships can be better understood enabling a more collaborative environment where systems work together for their mutual benefit. When a SoS is recognized, SoS managers and systems engineers can work collaboratively with the managers and systems engineers of the component systems to leverage and influence the development of those systems to address unique SoS needs. It allows the SoS systems engineers to focus on those areas that are critical to the SoS success and to leave issues related to the component systems to the systems. A SoS approach allows the FAA to leverage new or existing systems to provide needed and unique functionality to fulfill a common operational need. This approach results in a SoS capability greater than the sum of the capabilities of the constituent parts.

1.5.2 Integration Challenges

A SoS can evolve as a new system is developed; this new system may depend on inputs or functions being provided by existing systems or on another system that might be developed in another timeframe. If a new system allocates functional requirements to an existing system, that existing system needs to ensure that the new requirements do not adversely impact its current functions. The impact on the overall

system capacity and reliability needs to be determined to verify that the new and legacy functions are performed to specification requirements and are fully compatible. Specialized testing may be required.

In general, it is more difficult to test and assemble a SoS than a single system due to the diverse, autonomous constituent systems that make up the SoS. At a minimum, risk mitigation, testing, and validation can be expected to be largely distributed. Ongoing research is attempting to determine appropriate testing and validation methods. Aspects such as security, safety, assurance, reliability, availability, integration risks, and net-centricity need to be reassessed for the SoS. While the constituent systems may meet all assurance requirements, the networking of these systems into a SoS may introduce new vulnerabilities.

1.5.3 Additional Information

Since SoS considerations affect a number of systems engineering activities, additional information regarding SoS considerations are included within a number of sections in this document. The following sections within this document contain information specific to SoS within the FAA:

- Requirements Analysis
- Architectural Design Synthesis
- Risk Management

A detailed explanation on how to identify a System of Systems and ensure that the necessary systems engineering activities are accomplished to accommodate the added complexity can be found in Appendix A: Special Considerations for System of Systems.

Additional Information

For sources of information used to generate content throughout this section, see References.

To learn more about the topics in this section, see Additional Tools and Reading Recommendations.

2 Systems Engineering and the AMS Lifecycle

The FAA Acquisition Management System (AMS) was established in 1996 to address the unique needs of the agency and provide for more timely and cost-effective management of investments in equipment, materials, and services. This policy covers many management disciplines, including strategic planning, budgeting, enterprise architecture, portfolio management, and investment decision-making. Further information on acquisition management policy is available on-line via the FAA Acquisition System Toolset (FAST).

2.1 AMS Lifecycle Management

FAA systems engineers are most concerned with developing solutions to meet stakeholder needs. At certain points during this development process, the solution must be evaluated by management and approval authorities in order to justify continuing development and investment. A typical investment program within the AMS undergoes a lifecycle that is represented in Figure 3. The diagram depicts an evolution that begins with identified service needs, continues through stages of analysis and solution development, and culminates in a solution that is put into service until such time as it is replaced or updated. This section of the SEM provides a systems engineering perspective on how a solution – a program, system, or investment – passes through the various stages of the lifecycle. Another critical element of FAA systems engineering is applying the "system of systems" principles discussed in Section 1.5 to multiple interconnected, complex, asynchronous programs.

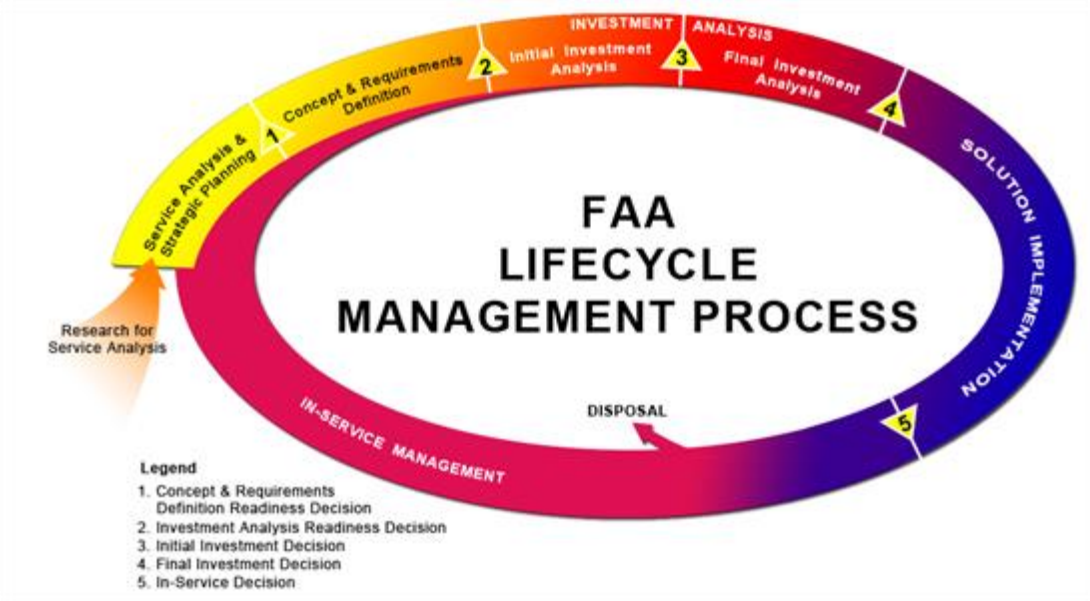


Figure 3: FAA Program Lifecycle Management within AMS

As a management process that is formalized in FAA policy, the AMS life cycle contains a number of formal decision points that define the status of agency investment initiatives. They are represented by the numbers in Figure 3. Each decision point requires the completion of an array of activities specific to the phase and the approval of a documentation package that summarizes those efforts. The documents reflect the maturity of the program's requirements, planning, and development processes. Systems engineering plays a critical role in facilitating and ensuring program flow through the life cycle, resulting in a solution that satisfies the service needs in addition to other agency strategic objectives.

Each subsequent section details a life cycle phase and contains a table listing the required documentation for its concluding decision point. A broad description of the phases and their corresponding decision points are as follows:

Service Analysis & Strategic Planning – Identify and define service needs and align them with strategic objectives. Decision point (1) is the Concept and Requirements Definition Readiness Decision.

Concept and Requirements Definition – Research and analyze concepts that might satisfy identified needs; define functional and performance requirements; identify preliminary alternatives. Decision point (2) is the Investment Analysis Readiness Decision.

Investment Analysis – Refine requirements and analyze solution alternatives; solicit feedback from industry vendors; select option for investment. Sub-phases are Initial Investment Analysis and Final Investment Analysis. The decision points are (3) Initial Investment Decision and (4) Final Investment Decision.

Solution Implementation – Develop and produce the solution; deploy it in the field and commission it. Decision point (5) is the In-Service Decision.

In-service Management – Operate, maintain, and sustain the solution until it must be disposed of, updated, or replaced.

To gain another perspective on what each FAA life cycle phase constitutes, Figure 4 maps them to a generic product life cycle, such as described in ISO standard No. 15288 (2008). While each solution may be developed in a slightly different manner, this depiction provides a sound notional basis for relating an FAA solution to any other developmental product.

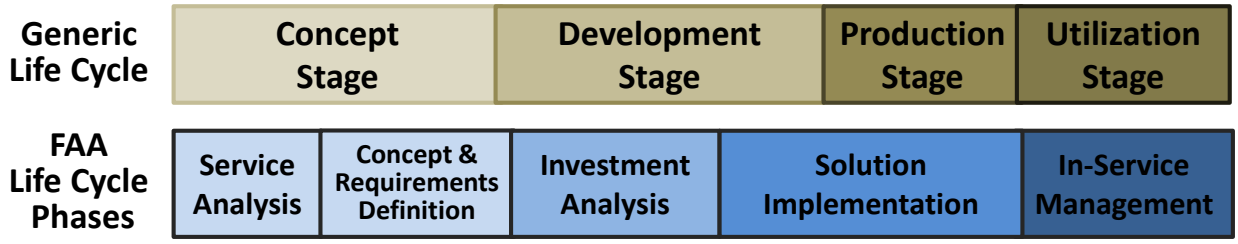


Figure 4: Mapping of Lifecycle Stages

In the sections that follow, each lifecycle phase is described from the perspective of systems engineering. Each section generally follows this format:

- **Phase diagram** – a quick reference to the primary inputs, activities, and outputs required, with a focus on systems engineering
- **Activity descriptions** – the systems engineering efforts required to synthesize the inputs, coordinate with other entities, and prepare documentation packages for management decision points
- **Phase products –** a table that shows the various artifacts that are created in support of phase activities and decision point deliverables. Some items may not be mentioned in the activity descriptions, such as artifacts that do not require systems engineering support.

It is important to note that systems engineering is a skill set that is represented in members of a given project team. Activities described as part of the lifecycle phases often support the project manager and may be assigned to any team member(s); the reader should not assume that everything listed in this section is a task for systems engineers only. Section 3: Systems Engineering Processes details the activities and processes that are more specific to a systems engineering role.

2.2 Phases of the AMS Lifecycle Management Process

The first official phase of the AMS lifecycle management process is Service Analysis and Strategic Planning. It should be noted that prior to the AMS policy update in April 2013 it was called Service Analysis. This initial phase establishes the basis for long-range strategic planning by individual service organizations and the FAA as a whole. The objectives of this lifecycle phase and the following one – Concept and Requirements Definition (CRD) – are to identify a capability shortfall, quantify a need, and identify potential technological opportunities to address that need.

However, as shown previously in the AMS lifecycle graphic, Figure 3, there is a separate activity – Research for Service Analysis (RSA) – that occurs throughout a number of lifecycle phases, as needed. As its name implies, RSA primarily supports the objectives of Service Analysis and Strategic Planning. Since it is not an official AMS lifecycle phase, with its own decision point and required work products, the section has a slightly different format than those that follow.

2.2.1 Research for Service Analysis

RSA is sometimes required during service analysis to mature operational concepts, reduce risk, and define requirements before a decision is rendered to proceed in the lifecycle management process. RSA performs research and systems analysis activities that are needed to develop enterprise architecture products to meet the criteria to enter CRD. In addition, RSA supports AMS portfolio management policy when alignment across related initiatives is necessary to progress concepts through the lifecycle. This relates to the System of Systems concept introduced in Section 1.5.

Two distinct portfolios contribute analysis products to Research for Service Analysis:

- Research, Engineering & Development (RE&D)
- Concept Maturity and Technology Development (CMTD)

Research, Engineering & Development is a portfolio for the study of new concepts, products, and procedures with potential benefits for the aviation community, particularly in the areas of materials, human factors, and aviation medicine. These activities inform FAA strategic planning, the NAS Enterprise Architecture (EA), and CMTD activities, but do not lead directly to CRD. RE&D activity across FAA is coordinated through the RE&D portfolio process. The RE&D portfolio is developed each year using strategic planning in the National Aviation Research Plan as a guide. This plan links FAA research activities to broader strategic planning in the NAS Concept of Operations (ConOps), NextGen Implementation Plan, the NAS Enterprise Architecture, and the Joint Planning Development Office.

Concept Maturity and Technology Development efforts include concept feasibility studies, technical analysis, prototype demonstrations, and operational assessments that identify, develop, and evaluate opportunities for improving the delivery of NAS services. These efforts reduce risk, define and validate requirements, identify and characterize safety hazards, inform CRD activities, and generate information that supports agency investment decisions and product lifecycle management. CMTD activities may be applied to a single initiative or multiple initiatives related to a single concept, i.e., a portfolio. They often play a role in the development of work products for the Service Analysis and Strategic Planning phase. Key outputs are mature, validated concepts that are strategically aligned with agency objectives and may be included in the NAS ConOps and FAA Enterprise Architecture and then enter the CRD phase. Refer to the *Concept Development and Validation Guidelines* for additional information and guidance on CMTD activities and methodologies. Section 3.1: Operational Concept Development provides additional detail on the concept development and validation work that is performed as part of CMTD.

2.2.2 Service Analysis and Strategic Planning

The Service Analysis and Strategic Planning (SA&SP) phase determines what capabilities must be in place now and in the future to meet agency goals and the service needs of customers. Results are captured in the "as is" and "to be" states of the FAA enterprise architecture, as well as the strategic roadmaps for moving from the current to the future state. Continuing analysis keeps planning current with changes in the service and operational environments.

Industry best practices – technology and service demand forecasting, portfolio management, customer surveys, for example – are employed during SA&SP to align service outcomes with the activities necessary to realize benefits for the FAA and its customers. SA&SP may lead to the refocus, reduction, or elimination of ongoing investment programs, and may identify new and more productive ways of doing business. As described previously, some investment opportunities may require early research and development – via RSA – to demonstrate operational concepts, reduce risk, or validate requirements before proceeding further in the lifecycle management process.

Service Analysis develops a qualitative, preliminary description of the priority service need, existing legacy assets, and the capability shortfall. Service Analysis may also be conducted for important service needs not within an EA roadmap as the basis for determining whether to add them. Systems engineers participate actively in these analysis and planning tasks.

Strategic Planning refers to an enterprise-level management process that analyzes agency objectives and the investment needs of each service organization in order to create an investment framework for the FAA and formulate a long-term plan that achieves the agency's mission. These planning activities translate strategic goals into high-level courses of action for service organizations and evolve the strategic direction of the FAA over time as the operating environment changes. Systems engineering also plays an active role in planning activities. They are summarized here to provide context for how the agency establishes and matures a concept for potential investment, but a more detailed description can be found in the AMS policy pages on the FAST website. Note: the term "service organization" can be somewhat complicated, and is defined thoroughly in section 1.2.3 of the AMS policy.

Figure 5 illustrates the process by which the agency determines and prioritizes its service needs that may eventually require investment. SA&SP activities provide an annual update to the FAA Enterprise Architecture, NAS ConOps, and other top-level strategy documents. The Enterprise Architecture roadmaps specify when identified service needs or shortfalls are planned to enter the AMS lifecycle management process for resolution and highlight interdependencies between investments. Destination 2025 establishes long-term strategic and performance goals for the agency.

Figure 5: Service Analysis and Strategic Planning Phase Diagram

Activity Descriptions

The Service Analysis and Strategic Planning phase consists of several activities which the systems engineer must perform, support, and track. These activities are described below in more detail, and occur in roughly this order, although some amount of overlap and iteration is frequently necessary.

A. *Describe Priority Need and Preliminary Shortfall*

Service organizations analyze forecasts for aviation service needs as one basis for determining and prioritizing service needs and shortfalls. A continuing dialogue with customers is also contributory. When a previously-approved EA roadmap specifies that a new service need is an agency priority, the responsible service organization then defines the capability that will improve service delivery and achieve agency strategic and performance goals. The service organization also describes any legacy assets or existing systems, facilities, people, and processes that currently perform the function or service. With this information, the service organization defines the service shortfall and the difference between future service need and current capability as a foundation for understanding the nature of the problem and its urgency and impact. The differences between future service needs and current capability is documented in the Preliminary Shortfall Analysis Report. For further guidance and templates, see the *Shortfall Analysis Guidelines.*

Systems Engineering Role: The systems engineer works with operational specialists to define and describe the preliminary service need, legacy assets, and the infrastructure shortfall. Systems engineering helps to identify business, technology, organizational, process, and personnel issues that affect service outcomes, as well as assumptions, risks, and dependencies.

B. Propose Enterprise Architecture Changes

For important, new capabilities not already contained in the FAA Enterprise Architecture, the service organization prepares a change notice reflecting the service need or shortfall and submits it to the FAA Enterprise Architecture Board for endorsement. A program or capability must be included in an Enterprise Architecture roadmap in order to successfully complete the following phase, Concept and Requirements Definition. Service needs and shortfalls are expressed as Operational Improvements. In addition, when a service shortfall impacts the NAS, strategic planning must be performed to ensure that the NAS ConOps evolves in accordance with the analyses of service demand and operational needs. This update and decomposition process is described in more detail in AMS policy, section 2.3.1.

Systems Engineering Role: The systems engineer develops solution-level architectural products necessary to support Enterprise Architecture changes. At the enterprise or NAS level, systems engineering supports the process of updating the NAS ConOps and other strategic planning documents to reflect forecasted service needs and shortfalls.

C. Perform Initial Safety Review

An integrated safety assessment serves to identify hazards arising from interacting initiatives. It helps define the program scope to eliminate safety gaps within a capability or service and to prevent new safety gaps from being introduced. Safety assessment for FAA programs is guided by the *SMS Manual* and the *Safety Risk Management Guidance for System Acquisitions* (SRMGSA); these may be available from the FAA website.

Systems Engineering Role: The systems engineer performs or supports the safety review, depending on the engineer's experience with safety assessments and the size of the initiative being analyzed.

D. Prepare Concept and Requirements Definition (CRD) Plan

The CRD Plan specifies the tasks of Concept and Requirements Definition and how they will be accomplished, defines the roles and responsibilities of participating organizations, defines outputs and exit criteria, establishes a schedule for completion, and specifies needed resources. FAA Systems Engineering and Safety and Investment Planning and Analysis works with the responsible service organizations to assist in the preparation of this plan. Organizations that sign the CRD Plan agree to provide the necessary resources.

Systems Engineering Role: The systems engineer ensures that sufficient engineering resources and time are included in the CRD Plan.

Table 2 summarizes the work products that are used and developed in the Service Analysis and Strategic Planning phase. For more details on these artifacts and other aspects of this phase, use the references in Section 6.

Table 2: Service Analysis and Strategic Planning Work Products

Product	Description	Supporting Processes
Validated FAA need or opportunity	A validation that the expressed need is traceable to an approved FAA enterprise document or ConOps	• Operational Concept Development • System Safety Engineering
Preliminary Shortfall Analysis Report	Describes qualitatively the service need, shortfall, and legacy assets that perform functions	• Functional Analysis • Decision Analysis
Initial functional requirements	Initial high-level analysis of needed functionality	• Functional Analysis • Requirements Analysis
Enterprise Architecture change notices	The recommended changes to the enterprise architecture to accommodate the planned initiative. This ensures that it is on a strategic roadmap.	• Interface Management • Systems Engineering Information Management
Risk Assessment	Initial Risk Status	• Risk, Issue, and Opportunity Management
Configuration Management Plan	The initial configuration management plan	• Configuration Management
Integrated Safety Asseessment	Early identification of safety gaps and hazards that may arise from concepts that interact with other systems.	• System Safety Engineering
Concept and Requirements Definition (CRD) Plan	A plan for accomplishing the CRD phase.	• Integrated Technical Management
*Note: **Bolded** items are required as inputs to CRD.*		

2.2.3 Concept and Requirements Definition

The Concept and Requirements Definition (CRD) phase accomplishes three primary tasks:

- Translate priority operational needs into a Concept of Operations document
- Quantify the service shortfall in order to define a functional architecture and preliminary requirements
- Identify the most promising alternative solutions and estimate the associated rough order of magnitude costs

Planning for CRD typically begins when an enterprise architecture roadmap specifies that a priority service or infrastructure need must be addressed. These needs typically relate to existing or emerging shortfalls in the "as is" architecture or essential building blocks of the "to be" architecture. Solutions that are not generated from a roadmap in this way require the development of architectural change products and amendments before obtaining endorsement from the FAA Enterprise Architecture Board.

Figure 6 summarizes the essential inputs, activities, and outputs of the CRD phase in the AMS lifecycle management process. They are required to advance a solution toward obtaining investment funding in the subsequent phase. Additional details on CRD activities can be found in *CRD Guidelines*, from the FAA website.

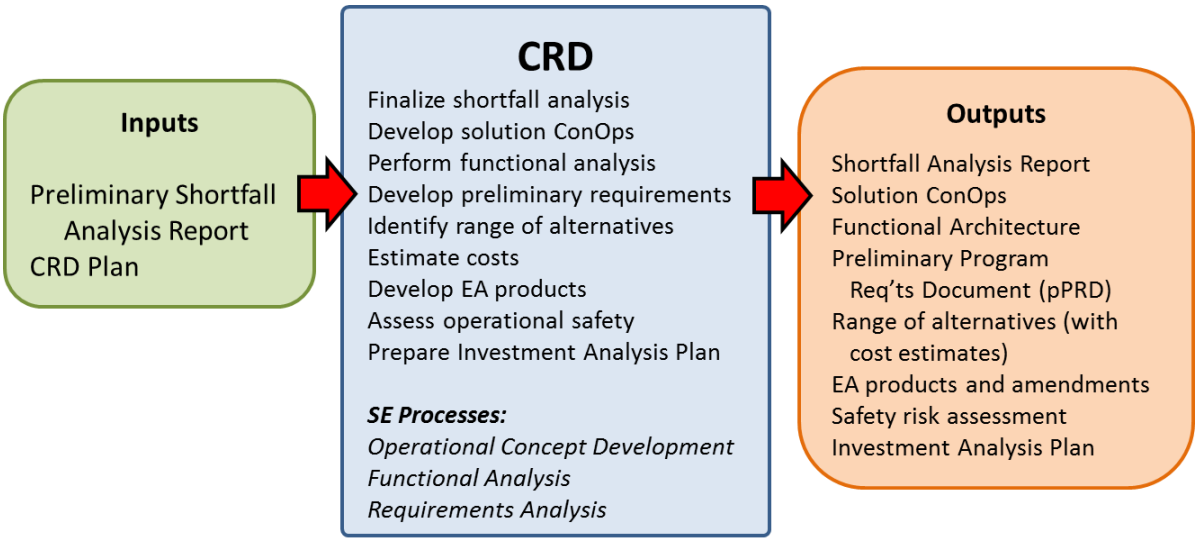


Figure 6: Concept and Requirements Definition Phase Diagram

Activity Descriptions

CRD consists of many activities which the systems engineer must either perform, support, or track. These activities are described below in more detail, and occur in roughly this order, although a fair amount of overlap and iteration is frequently necessary.

A. Finalize Shortfall Analysis

The service organization or program office updates, refines, and quantifies the preliminary shortfall identified during service analysis in sufficient detail to serve as the basis for (1) clearly understanding the nature, urgency, and impact of the service need; (2) defining preliminary requirements; (3) determining realistic and economic alternative solutions; and (4) quantifying likely ROM program costs and benefits. **Systems Engineering Role:** The systems engineer takes the lead in quantifying the service shortfall in a detailed Shortfall Analysis Report.

B. *Develop a Solution Concept of Operations*

The solution Concept of Operations describes how users will employ the new capability within the operational environment and how it will satisfy the service need that was defined during the shortfall analysis. The solution ConOps:

- Defines the roles and responsibilities of key participants (e.g., controllers, maintenance technicians, pilots)
- Explains operational issues that systems engineers must understand when developing requirements
- Identifies procedural issues that may lead to operational changes
- Establishes a basis for identifying alternative solutions and estimating their ROM costs

This document serves as the foundation for subsequent functional analysis and the development of preliminary requirements. The systems engineering process described in Section 3.1, Operational Concept Development, is essential to developing the ConOps.

Systems Engineering Role: The systems engineer is the technical lead for development of the solution ConOps. The systems engineer is also responsible for validating that the ConOps fulfills the service capability specified in higher-level NAS ConOps and the Shortfall Analysis Report.

C. *Perform Functional Analysis*

Functional analysis translates the service needs identified in the shortfall analysis and NAS ConOps into high-level functions that must be performed to achieve the desired service outcome. This process then decomposes high-level functions into lower-level sub-functions. The outcome is a functional architecture that serves as a framework for developing requirements and the subsequent physical architecture. It is important that the definition of functions focuses on what the new capability will do and not *how* the service will be provided.

Systems Engineering Role: The systems engineer leads this activity, which in addition to the functional architecture may include development of N^2 diagrams, functional flow block diagrams, and other functional analysis outputs. For further explanation, see Section 3.2, Functional Analysis.

D. *Develop Preliminary Program Requirements*

Preliminary Program Requirements (pPR) are based on the functional architecture and define the high-level functions and performance that will satisfy the identified service needs. Interface, safety, security, and other constraint requirements may also be part of pPR development. Preliminary requirements must be solution agnostic; they should be written to allow unbiased and measurable evaluation of various solution alternatives. Concept development and validation activities such as analysis, modeling, simulation, and prototyping may be necessary to adequately define some requirements. These activities are generally performed as part of the Concept Maturity and Technology Development portfolio.

Systems Engineering Role: Developing preliminary requirements is an iterative, collaborative effort that relies on multiple technical and programmatic disciplines and mustalso involve users and stakeholders. The systems engineer communicates with stakeholders and subject matter experts to ensure that all preliminary requirements are traceable to the functional architecture and also are coordinated with the enterprise architecture products that are often developed concurrently. For more detail on this critical systems engineering process, see Section 3.3, Requirements Analysis.

E. *Identify Range of Alternatives*

Developing a range of distinct alternative solutions increases the likelihood that the best possible one will be selected to satisfy the service need or eliminate the capability gap. Key factors are safety, security, operational cost efficiencies, technological maturity, and impact on the workforce and enterprise architecture. Alternatives must be qualitatively different, and some may not meet

100% of the preliminary requirements. Non-material solutions such as procedural, personnel, or policy changes should also be considered. Some sources for solutions include trade studies, vendor-supplied concepts, and modification of legacy assets. The service organization produces technical descriptions for a minimum of three distinct solutions.

Systems Engineering Role: The systems engineer identifies solution alternatives from existing systems (or systems in development) that could contribute functionality required to meet the identified shortfalls. The systems engineer ensures that all proposed alternatives are compatible with the NAS ConOps and high-level NAS requirements documentation. The systems engineer plays a key role in writing the technical descriptions, assessing technological maturity of solutions, and identifying trade-offs among alternatives.

F. Estimate ROM Costs

Rough lifecycle costs are developed for each alternative and compared to the monetized shortfall as a basis for determining whether it should be retained or eliminated from consideration. Rough lifecycle costs are also calculated for sustaining the legacy case in service. This provides a basis for determining whether an alternative should be investigated further or eliminated from consideration. The technical descriptions formulated in the previous activity serve as the basis for estimating ROM lifecycle costs.

Systems Engineering Role: The systems engineer ensures that all activities for supporting the solution throughout its lifecycle are considered and accounted for in the cost estimate. This includes such items as deployment and transition, integrated logistics support, technology sustainment and evolution, and disposal of any assets that would be replaced. The systems engineer also ensures the set of preliminary requirements can be tied to a collection of tangible benefits.

G. Develop Enterprise Architecture Products

Solution-level enterprise architecture products are “snapshots” of a solution at particular points in time. They show the “as-is” and the “to-be” states of the Enterprise Architecture (EA). Products required during CRD depict specific relationships and summarize information contained in the solution ConOps and the Preliminary Program Requirements for each of the alternative solutions to be evaluated. This includes the high-level operational concept, a dictionary of architectural elements, a functional hierarchy, and an activity hierarchy, among others. While pursuing solution initiatives, system experts or systems engineers may find EA elements that need to be amended to accommodate the planned architecture. They should fully document the recommended changes and create a revised NAS EA product to reflect the proposed amendment or change, as well as justify the changes.

Systems Engineering Role: The systems engineer supports both the enterprise- and solution-level architects in developing required enterprise architecture views and ensuring that the EA products are properly integrated both horizontally (across solution-level architectures) and vertically (clearly linked from the enterprise-level to solution-level.) Systems engineers are uniquely qualified to apply a system-of-systems perspective to all proposed solutions; this may include the identification of capabilities that are shared among various systems; these must be coordinated but not duplicated. Additional description of EA activities can be found in Section 3.4, Architectural Design Synthesis.

H. Assess Operational Safety

When an initiative enters the AMS lifecycle, its impact on the NAS and system safety must be assessed in accordance with guidance found in the Safety Management System (SMS) Manual. If the solution may impact the safety of the NAS, a Safety Risk Management Document (SRMD) must be developed at each of the principal AMS decision points. The goal is to ensure the safety of the NAS by identifying system risks and associated mitigations as early as possible. Depending on whether a given solution affects NAS safety, the relevant safety organization either performs an Operational Safety Assessment (OSA) or issues a Safety Risk Management

Decision Memo. The need to mitigate identified safety risks often results in the addition of safety requirements to the Preliminary Program Requirements Document.

Systems Engineering Role: The systems engineer supports the safety team by supplying information on the functions and capabilities of proposed solution alternatives. Depending on experience and the size and complexity of the initiative, systems engineers may perform or support the safety assessment and produce the resulting documentation.

I. Prepare Investment Analysis Plan

Preparations for the next phase commence once the solution ConOps, preliminary requirements, functional architecture, EA products, and safety assessments have been fully validated to ensure that the proposed solutions will satisfy the identified shortfall or service need. At this point, an Investment Analysis Plan is developed to ensure resources are in place to complete the requirements of the IA phase. The plan for investment analysis: (1) defines scope and assumptions; (2) describes alternatives and their associated rough lifecycle costs; (3) describes planned activities and specifies how tasks will be accomplished; (4) defines output and exit criteria; (5) establishes a schedule for completion; (6) defines roles and responsibilities of participating organizations; and (7) estimates resources needed to complete the work.

By signing the Investment Analysis Plan, the organizations that will conduct the analysis agree to provide the resources necessary to complete the work. The *Investment Analysis Plan Guidelines* document provides a template and further guidance on this activity.

Systems Engineering Role: The systems engineer ensures that sufficient engineering resources are included in the plan to complete the SE tasks in the subsequent investment analysis activities.

Other Systems Engineering Responsibilities

The systems engineer helps to:

- Develop requirements and evaluate preliminary solution alternatives with regard to specialty engineering disciplines such as safety; reliability, availability, and maintainability; human factors; electromagnetic compatibility and interference; information security; and environmental impact. These disciplines also contribute to defining preliminary functional and performance requirements and eliminating alternatives that have unacceptable negative attributes.
- Validate that the solution ConOps is aligned with the NAS ConOps

Identify and mitigate technical risks that emerge during CRD

Table 3 summarizes the work products that are used and developed in the Concept and Requirements Definition phase. For more details on these artifacts and other aspects of CRD, use the references in Section 6.

Table 3: CRD Work Products

Product	Description	Supporting Processes
Preliminary Program Requirements Document (pPRD)	High-level functional, performance, interface, safety, security, and constraint requirements that must be solution-agnostic	• Requirements Analysis • System Safety Engineering • Verification & Validation
Solution Concept of Operations (ConOps)	How the proposed solution will satisfy the service need and work with existing and planned assets.	• Operational Concept Development • Verification and Validation

Product	Description	Supporting Processes
Final Shortfall Analysis Report	Serves as the basis for (1) clearly understanding the nature, urgency, and impact of the service need; (2) defining preliminary requirements; (3) determining realistic and economic alternative solutions; and (4) quantifying likely program costs and benefits.	• Functional Analysis • Decision Analysis
Functional Architecture	Translates service needs into high-level functions that must be performed to achieve the desired service outcome in every operating environment in which the solution will perform.	• Functional Analysis • Architectural Design Synthesis
Operational Safety Assessment (OSA)	Develops coordinated, systematic safety objectives and requirements for the overall solution (including procedural considerations) early in the development phase.	• System Safety Engineering
Operational Services and Environment Definition (OSED)	Describes the modes of operation and intended operational environments for a proposed solution	• Functional Analysis • Requirements Analysis • Information Security Engineering
Enterprise Architecture products and amendments	EA products (e.g., “views”) that are built during CRD. The Integrated Systems Engineering Framework (ISEF) provides guidance on which products are needed for a given initiative.	• Architectural Design Synthesis • Interface Management • Systems Engineering Information Management
Realistic alternatives	Preliminary range of alternatives with descriptions, including pros and cons for each. May include monetized shortfall estimates.	• Operational Concept Development • Functional Analysis • Requirements Analysis • Integrated Technical Management
Rough order of magnitude cost estimate for each alternative	Provides more precision than the cost estimate produced in Service Analysis.	• Functional Analysis • Requirements Analysis
Operational Capability Integration Plan (OCIP)	Plans how each investment increment will integrate with other increments in the capability portfolio and the FAA Enterprise Architecture.	• Integrated Technical Management
Systems Engineering Management Plan (SEMP)	Plans the systems engineering efforts – personnel and tasking – required to progress the given initiative through the anticipated milestones and decision points, including vendor oversight activities. As an optional work product, the systems engineer and/or program manager make a judgment as to whether the program is sufficiently complex to require a SEMP. Can be initiated during any phase of solution development.	• Integrated Technical Management

Product	Description	Supporting Processes
ACAT designation request	The ACAT is based on dollar thresholds as well as qualitative factors such as program risk, complexity, political sensitivity, and likelihood of changes to the safety of the NAS.	• Integrated Technical Management
(Initial) Investment Analysis Plan	A plan for accomplishing the Initial Investment Analysis phase. Ensures that sufficient resources are in place to complete IIA requirements.	• Integrated Technical Management • System Safety Engineering
*Note: **Bolded** items are required as inputs to Initial Investment Analysis*		

2.2.4 Investment Analysis

Investment Analysis is a disciplined process that supports sound capital investment decisions. In deciding which capital investments the Agency will fund, FAA executives consider many investment proposals from multiple service organizations in competition for a limited capital investment pool. Investment analysis is conducted in the context of the enterprise architecture and FAA strategic goals and objectives. The key is to balance timeliness, complexity, and size of the investment analysis with the rigorous development of quantitative data needed by the investment decision authority – the Joint Resources Council – to make an informed final investment decision. The level of effort required during this phase is directly proportional to the size and complexity of the potential investment, as reflected by the Acquisition Category (ACAT) designation as well as the number of interrelated investments and capabilities that it impacts.

In essence, Investment Analysis develops convincing evidence of two things:

- The investment proposal is the most attractive economic investment opportunity available to the FAA and its customers, and
- The plan for implementing and operating the investment is well-conceived, low-risk, well-documented, and well-understood within the FAA and industry.

Given these objectives, the Investment Analysis consists of two phases:

- **Initial Investment Analysis** generates the information needed to select the alternative offering the most promising solution to the service shortfall
- **Final Investment Analysis** develops detailed cost and benefits estimates, plans, and final requirements for the selected alternative

As a fundamental component of systems engineering, requirements development is often viewed as representative of a solution's maturity. Throughout the course of Investment Analysis, an investment analysis team advances the state of program requirements as shown in the top half of Figure 7. Of equal importance during Investment Analysis, however, is the interaction with potential solution vendors via the contracts process, as shown in the bottom half of the diagram. Feedback from industry is critical to informing requirements development and ensuring that all available technologies are considered to achieve the desired solution. The following sections detail the activities undertaken within each sub-phase to refine and evaluate the potential investment. Additional details on IA activities can be found in *Investment Analysis Process Guidance*, a document published by the Office of Investment Planning and Analysis, which can be found on FAST.

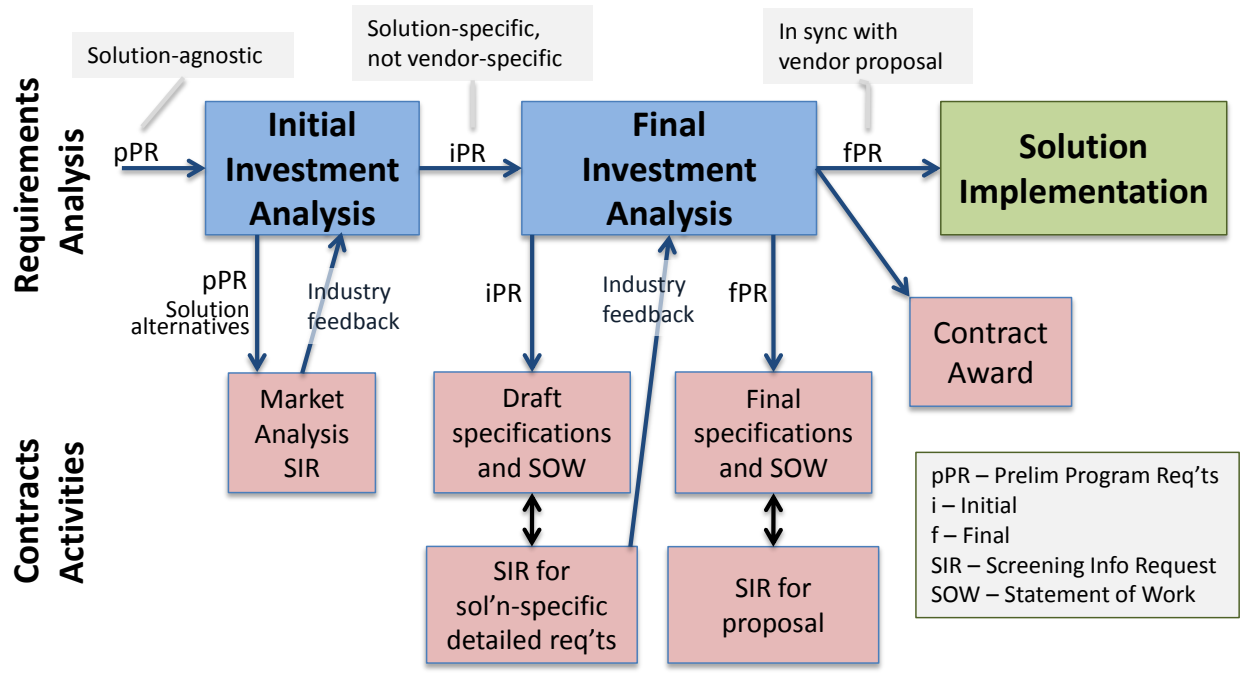


Figure 7: Requirements and Contracts Interactions in Investment Analysis

2.2.4.1 Initial Investment Analysis

The objective of Initial Investment Analysis (IIA) is to determine the best solution by analyzing feasible alternatives within the context of their economic, operational, performance, budgetary, and risk constraints. IIA applies only to New Investment decisions. Other investment types – such as Tech Refresh and Variable Quantity – proceed directly to Final Investment Analysis.

Figure 8 summarizes the essential inputs, activities, and outputs of the Initial Investment Analysis phase in the AMS lifecycle management process.

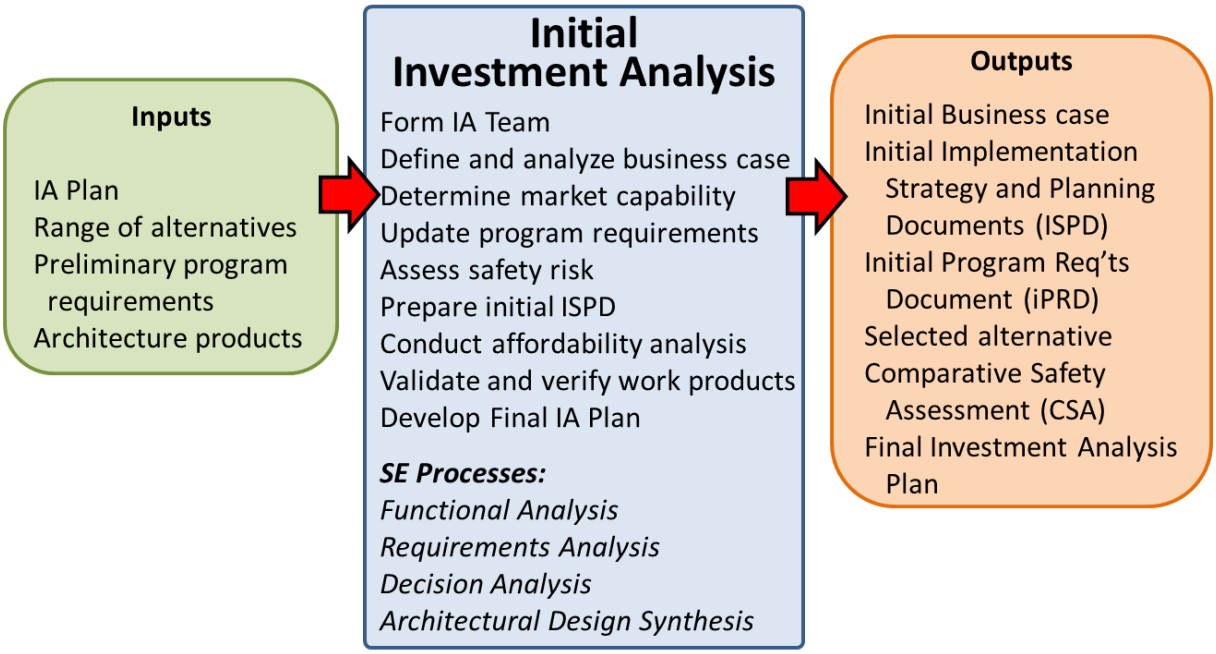


Figure 8: Initial Investment Analysis Phase Diagram

Activity Descriptions

IIA consists of many activities which the systems engineer must either perform, support, and track. These activities are described below in more detail, and occur in roughly this order, although a fair amount of overlap and iteration is typical.

A. Form Investment Analysis Team

The Investment Analysis Plan developed during CRD outlines the membership of the investment analysis team. The team is formed and scaled to the size and complexity of the anticipated analysis. The team reviews the plan and makes any needed adjustments, such as to the schedule and team composition. The team leader requests from management any additional members needed to perform the tasks and complete the products of IIA within the specified timeframe. Membership is from a variety of functional disciplines, including operational subject matter experts, systems engineers, enterprise architects, logistics specialists, and analysts from the Investment Planning and Analysis Directorate. Specialty engineering personnel and security and regulatory specialists are included when required by the particular investment type.

Systems Engineering Role: The systems engineer must ensure that sufficient engineering resources are available to the team to complete the IIA activities and work products. This may involve establishing commitments from a range of specialty engineering disciplines and support organizations. For smaller programs, a systems engineer may need to perform or support a range of activities that lie outside those considered typical for systems engineering.

B. Define and Analyze Business Case

Defining the business case and associated metrics is essential for determining what information must be gathered and analyzed during IIA to select the best solution alternative for the service need or shortfall. A business case focuses on the factors that demonstrate the value and worth of a proposed investment program to the FAA and its customers. Key factors include the impact on and contribution to FAA strategic goals; alignment with the FAA enterprise architecture; contribution to the service needs of customers; impact on essential FAA mission responsibilities; and risk. Of equal importance are lifecycle costs and benefits – particularly the potential for

lowering operational costs, reducing system delays, and improving flight efficiency and safety. Additional guidance for defining and analyzing the business case may be found at the Investment Planning & Analysis (IP&A) website and on FAST.

The business case is supported by the following engineering assessments: requirements sensitivity, technological maturity, architecture impact, and specialty engineering. Other factors that may be evaluated as part of a business case include interdependencies with other existing or proposed programs, supportability concerns, upgrade potential, and the time required to field a given capability. Some developments from the business case analysis are used throughout the Solution Implementation and In-Service phases, to track variances and proactively identify issues. The *Business Case Analysis Guidance* document at the IP&A website, and FAST, provides useful instruction and a template for this activity.

Systems Engineering Role: The systems engineering role during business case definition and analysis is substantial and complex. The business case must take into account new capabilities that may be split into multiple increments that proceed through the AMS lifecycle phases separately. As a result, the pacing and timing of a capability's enabling technologies are important concerns for the systems engineer who is defining the business case. Based on experience and research into comparable past acquisitions, a systems engineer may need to illuminate cost and schedule details for efforts that are far into the future and not yet fully developed.

The systems engineer may be called upon to lead, perform, and support any of the following four assessments that help mature a solution's business case:

- Requirements Assessment: Identify key requirements that drive costs and benefits. Analyze sensitivity of requirements with respect to cost and capability. Rank alternatives against Critical Performance Requirements and their impact on targeted FAA performance measures. Determine if business process re-engineering can reduce or relax requirements or lower costs.
- Technological Maturity Assessment: Review the technological maturity of each alternative and assess associated risks to cost, performance, and schedule.
- Architecture Impact Assessment: Describe how the investment opportunity supports the FAA Enterprise Architecture, including the enterprise-level roadmaps and architecture views.
- Specialty Engineering Assessment: Ensure that the following specialty engineering topics are integrated into the overall assessment of alternatives: Reliability, maintainability, and availability; radio frequency management; environmental impact; supportability and integrated logistics support; quality assurance and performance; enterprise configuration management and operations. The specialty engineering assessment includes the following three sub-assessments:
  - Human Factors Engineering and Operability Assessment: Analyze the full range of human factors and interfaces necessary to achieve an acceptable level of performance for operating, maintaining, and supporting the solution over its service life. For additional detail, reference *Human Factors Assessments in Investment Analysis: Definition and Process Summary for Cost, Risk, and Benefit*.
  - Information Security Assessment: Ensure that information technology security requirements and lifecycle costs are identified, assessed, and validated.
  - Environment and Occupational Safety and Health Assessment: Ensure that safety-related items on the investment decision authority readiness checklist have been completed.

C. Determine Market Capability

The standard means for gathering market capability data on potential solutions is a Screening Information Request (SIR). The initial SIR conveys FAA needs in the form of preliminary requirements and serves to determine industry interest in providing the eventual solution.

Subsequent requests seek successively more specific information as requirements mature throughout the investment analysis process. The market search focuses on industry and other sources with potential solutions -- government agencies, foreign institutions, and universities. Market research findings are documented as part of the business case package. More detail on the SIR process and other IA activities is available from the FAA Investment Planning and Analysis office.

Systems Engineering Role: Systems engineers may be called upon to perform market research or conduct trade studies to determine the technologies or techniques best suited to satisfy the program requirements. The systems engineer may help gather and screen technical responses from industry.

D. Update Program Requirements

The investment analysis team assesses vendor responses against preliminary requirements to determine whether relaxation or modification would enable promising concepts to be acceptable for implementation. The objective is to identify solutions that are diverse, innovative, and have a positive impact on targeted FAA performance without compromising essential stakeholder needs. At the end of IIA, the next step in requirements development and validation occurs when the investment decision authority approves Initial Program Requirements Document (iPRD); this document reflects industry input and is compatible with the selected alternative being proposed for investment. Additional guidance on requirements analysis, management, and documentation is available in Section 3.3, Requirements Analysis.

Systems Engineering Role: Using input from both stakeholders and vendor proposals, the systems engineer refines program requirements in order to lower cost or risk, or increase performance and benefits, while retaining critical performance of the range of potential solutions. Updates are also necessary to provide a more complete statement of functional and performance needs in order to guide responses to Screening Information Requests.

E. Assess Safety Risk

As a potential investment enters IA, system safety is assessed in accordance with guidance found in the Safety Management System (SMS) Manual. In IIA, this effort is focused on developing the Comparative Safety Assessment (CSA). Its goal is to compare alternate solutions from a safety perspective. The need to mitigate safety risks often results in the addition or modification of safety requirements in the Program Requirements Document.

Systems Engineering Role: Depending on experience and the size and complexity of the initiative, systems engineers may perform or support the safety assessment and produce the resulting documentation.

F. Prepare Initial Implementation Strategy and Planning Document

The Implementation Strategy and Planning Document (ISPD) is developed during Investment Analysis to describe the activities required to realize a particular solution. The document is based in part on industry feedback via Screening Information Requests, and may include factors such as: acquisition of systems and equipment, construction or modification of facilities and the physical infrastructure, functional integration within the Enterprise Architecture, and procurement of services. During IIA, the investment analysis team prepares an *initial* ISPD for each of the alternatives. These are not as detailed as the full ISPD that is developed later for the selected solution alternative, and the objective is to highlight any particular differences that would impact cost and schedule. Some examples include data rights, supportability issues, obsolescence, configuration management, and costs associated with use of Non-Developmental Items (NDI) or commercial off-the-shelf (COTS) components. The ISPD template located on the FAA website defines which sections are completed at this time. These initial plans form part of the basis for determining which alternative the investment decision authority should select. Additional information on completing the ISPD can be found in Section 4.1, Integrated Technical Management. If, due to its complexity, the program has already developed a SEMP, then the

ISPD is not needed and the SEMP is used going forward. This is a systems engineering decision.

Systems Engineering Role: The systems engineer defines the scope and complexity of systems engineering associated with each alternative, then estimates how the different architectures will impact such factors as cost, schedule, risk, reliability, maintainability, availability, configuration management, human integration, personnel requirements, documentation, interfaces, and specialty engineering. It is essential to determine when and how stakeholder buy-in will be obtained.

G. Conduct Initial Affordability Analysis

The investment analysis team forwards estimates of the lifecycle cost for each alternative to the Capital Investment Team. The Capital Investment Team assesses the budget impact of the proposed program and its relative contribution to satisfying FAA goals against other investment options and make a funding determination. When a solution cannot be funded within the capital investment program baseline, the Capital Investment Team may propose offsets from lower priority programs. Preliminary budget impact assessments by the Capital Investment Team will shape subsequent deliberations of the Investment Analysis Team.

Systems Engineering Role: Systems engineering is not directly involved in this analysis, but may be called upon to provide information that supplements life cycle cost estimates.

H. Validate and Verify Key Work Products

The primary focus of validation activities during IIA is to ensure that preliminary program requirements and the business case have been developed such that they describe a solution that meets the needs, gaps, and shortfalls defined by prior work. Work products are verified to ensure that all necessary data have been included, are correct, and conform to the relevant templates and guidance. Strict V&V leads to the selection of the best alternative for investment and eventual implementation. It essentially provides the investment decision authority with a “cross check” of the work performed and reduces risk associated with the investment decision. The *Business Case Assessment Guide* found on the IP&A website, provides additional details on business case validation.

Systems Engineering Role: Validation and verification is a key role of a systems engineer. Systems engineering also evaluates whether the degree to which each alternative satisfies program requirements is clearly expressed and supported by rigorous analysis. Requirement categories may include: performance, availability, compatibility, transportability, interoperability, reliability, maintainability, safety, human factors, logistics supportability, documentation, staffing, personnel, and training. These factors must be correctly specified in the updated program requirements document. Subject matter experts often assist in the validation activities, particularly with specialty functions or technologies.

I. Develop Final Investment Analysis Plan

The Final Investment Analysis Plan defines all work activities, resources, schedules, participating organizations, team members, roles, responsibilities, and products for the subsequent phase, Final Investment Analysis. It specifies entrance and exit criteria and a date for the Final Investment Decision. The FIA Plan calls out necessary risk-reduction activities such as analysis, modeling, simulation, or other research. It also includes procurement activity associated with the release of a Screening Information Request seeking vendor proposals for solution implementation. *Investment Analysis Plan Guidelines and Template* contains more details and instruction on this activity.

Systems Engineering Role: The systems engineer assists preparation of the plan, making sure sufficient engineering resources are included to complete such tasks as developing the product specifications and formulating Screening Information Requests.

J. Initial Investment Decision

When the business case is sufficiently mature, IIA results and recommendations are presented to the Joint Resources Council (JRC) for approval. The following items may need to be completed and socialized before this decision point: briefing materials and supporting documentation, readiness checklist, verification that exit criteria are satisfied, stakeholder coordination, identification of outstanding issues or concerns, briefing to the financial review authority, and a pre-brief of investment decision authority members.

Based on the program requirements, business case, and Implementation Strategy and Planning Document, the Initial Investment Decision selects the best alternative to proceed to Final Investment Analysis. TheJRC may also reject the alternatives and specify what alternate action is needed. The decision-makers determine which solution best contributes to FAA strategic and performance goals and provides the greatest economic benefit.

Systems Engineering Role: The systems engineer provides the basis for evaluating and selecting alternatives based on the decision criteria specified in AMS policy. Should the investment not be advanced to FIA, the systems engineer archives work products and drafts lessons learned. The role may also then involve re-work to propose an alternative with an improved cost-to-benefit ratio or other factors for a future effort to achieve the solution.

Table 4 summarizes the artifacts that are used or developed in the Initial Investment Analysis phase. For more details on these artifacts and other aspects of this phase, use the references in Section 6.

Table 4: Initial Investment Analysis Work Products

Product	Description	Supporting Processes
Initial Program Requirements Document (iPRD)	Updates the preliminary program requirements to provide a solution-specific statement of functional and performance requirements. Used to solicit market capability information from industry. Initial Program Requirements are *not* vendor-specific.	• Requirements Analysis
Enterprise architecture products and amendments	The enterprise architecture products that are built or updated during IIA. The ISEF provides guidance on which products are needed.	• Architectural Design Synthesis • Interface Management • SE Information Management
Comparative Safety Assessment (CSA)	Lists the hazards associated with a service change, along with a risk assessment for each alternative-hazard combination.	• System Safety Engineering
Recommended Alternative	Description of the solution alternative that best satisfies requirements and service shortfalls.	• Functional Analysis • Decision Analysis • Integrated Technical Management
Initial Business case	Captures the reasoning for initiating the potential investment. The underlying logic is that whenever resources are consumed, they support a specific business need.	• Integrated Technical Management • SE Information Management
Initial Implementation Strategy and Planning Document (ISPD)	Implementation strategy is the manner in which an organization plans to utilize organizational structure, control systems, and culture to develop and field the product or results of the project.	• Integrated Technical Management • Systems Engineering Information Management

Product	Description	Supporting Processes
Draft Program Statement of Work (SOW)	A detailed description of the specific services or tasks that a contractor is required to perform under a contract. SOW is usually incorporated in a contract.	• Functional Analysis • Decision Analysis • Integrated Technical Management
Operational Capability Integration Plan (OCIP)	How the selected alternative will integrate with other investment increments in the portfolio and the FAA Enterprise Architecture.	• Integrated Technical Management • SE Information Management
Final System Engineering Management Plan (SEMP)	The SEMP describes the contractor's technical approach and proposed plan for the conduct, management, and control of the integrated systems engineering effort.	• Integrated Technical Management • Systems Engineering Information Management
Final Investment Analysis Plan	A plan for accomplishing the Final Investment Analysis phase. Ensures that sufficient resources are in place to complete FIA requirements.	• Integrated Technical Management
*Note: **Bolded** items are required as inputs to Final Investment Analysis (FIA.)*		

2.2.4.2 Final Investment Analysis

The objective of Final Investment Analysis (FIA) is to mature the selected alternative into a low-risk, successful FAA investment program ready for solution implementation. This is accomplished through a set of integrated activities that focus on three goals:

- Reduce investment risk
- Begin procurement of the new asset
- Plan for solution implementation

Figure 9 summarizes the essential inputs, activities, and outputs of the Final Investment Analysis phase in the AMS lifecycle management process.

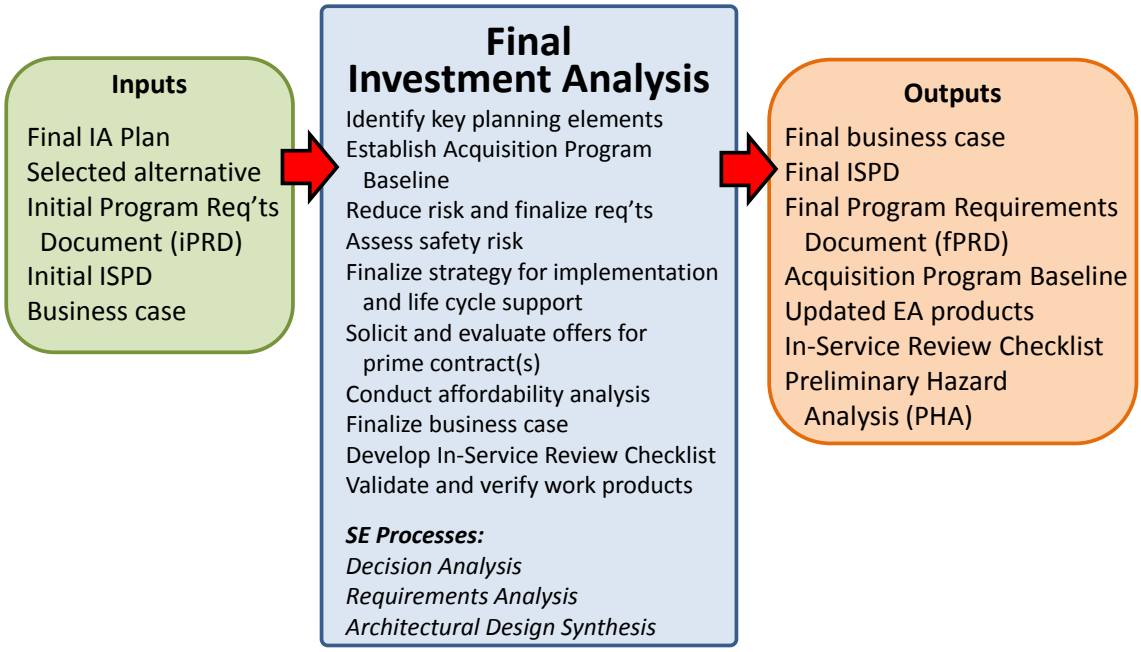


Figure 9: Final Investment Analysis Phase Diagram

Activity Descriptions

FIA consists of many activities which the systems engineer must either perform, support, or track. These activities are described below in more detail, and occur in roughly this order, although a fair amount of overlap and iteration is typical.

A. Identify Key Planning Elements

The investment analysis team identifies all actions and events necessary to obtain and support the solution over its lifecycle. This requires extensive coordination across the FAA to determine the full range of activities necessary to achieve efficient and effective lifecycle support for the solution and its operational assets. This includes logistics support, configuration management, test and evaluation, information security, system safety, human factors, physical infrastructure, and telecommunications. The team reviews and revises the Final Investment Analysis Plan accordingly.

Systems Engineering Role: The systems engineer ensures that sufficient engineering resources are available to complete the activities of FIA. This may involve establishing commitments from multiple engineering disciplines and organizations. The systems engineer also considers and

plans for the engineering activities required during the next phase, Solution Implementation. This may be shown in a preliminary Work Breakdown Structure (WBS) document.

B. Establish Acquisition Program Baseline

The Acquisition Program Baseline (APB) establishes cost, schedule, and performance targets to which the service organization charged with implementing a solution is held accountable and against which the program will be measured. It is the mutual agreement between the investment decision authority, the implementing service organization, and the user community concerning the performance and capability the program will provide and the authorized cost and schedule. The APB is finalized just prior to the Final Investment Decision (FID). The APB encompasses summary-level cost, schedule, and performance data from the final versions of the key FID artifacts: Final Program Requirements Document (fPRD), the final business case, and the final Implementation Strategy and Planning Document (ISPD). See the *FAA Acquisition Baseline Management Standard Operating Procedure* for further guidance.

Systems Engineering Role: After vendors respond to Screening Information Requests, the systems engineer uses those responses and the final business case to assist the implementing service organization develop accurate cost, schedule, and performance baselines for the APB.

C. Reduce Program Risk and Finalize Requirements

The investment analysis team performs a detailed examination of program risks that threaten performance, cost, schedule, and benefit objectives associated with the proposed solution. For example, simulations and prototypes may be developed by the relevant support organizations to evaluate concept feasibility, and an operational capability demonstration may provide feedback on the use of commercial, off-the-shelf components. The Acquisition Program Baseline includes risk mitigation costs and schedules.

After the completion of risk management planning and risk reduction activities, the final iteration of operational and performance requirements – including Critical Performance Requirements – are recorded in the Final Program Requirements Document (fPRD). The solution selected at IID must satisfy these requirements. Solution performance is evaluated against these measures during subsequent testing to determine operational suitability and effectiveness.

Systems Engineering Role: The systems engineer leads the activity to identify and assess technical risks associated with the solution and to define appropriate risk mitigation strategies. The outputs of this process are coordinated with stakeholders to achieve acceptance of resource and schedule recommendations as well as agreement on residual risk that will be carried into Solution Implementation for resolution.

The systems engineer leads a review of the solution functional baseline to ensure there is mutual agreement between the implementing service organization and operational stakeholders concerning the capability to be obtained during Solution Implementation. The systems engineer leads a review of the solution performance baseline to ensure that measures of overall performance are defined, cohesive and integral to the design and development process. Finally, the systems engineer leads a review of final program requirements to ensure they are completely and properly defined, and allocated to the proper technical specification or contract deliverable. This review establishes the final requirements baseline, the Final Program Requirements Document (fPRD).

D. Assess Safety Risk

The Safety Management System (SMS) Manual calls for a Preliminary Hazard Analysis (PHA) at this point in solution development. This report is more detailed than the previous OSA and CSA, as it is specific to the solution selected at Initial Investment Decision. Subsequent safety assessments continue to reflect the increasing maturity of the solution design. The need to mitigate safety risks may result in the addition or modification of safety requirements in the Program Requirements Document.

Systems Engineering Role: Depending on experience and the size and complexity of the initiative, systems engineering personnel may perform or support the safety assessment and produce the resulting documentation.

E. Finalize Strategy for Implementation and Lifecycle Support

The FAA standard work breakdown structure (WBS) serves as a basis for developing the overall strategy for procuring, deploying, operating, and supporting the solution over its service life. Within the WBS, tasks are described in sufficient detail that resources and schedules can be determined and recorded in the final business case and Acquisition Program Baseline documents. The final Implementation Strategy and Planning Document (ISPD) is the work product that includes this detailed strategy, as well as the roles and responsibilities of individuals and organizations critical to program success. Section 4.1: Integrated Technical Management includes additional guidance on program lifecycle planning.

System Engineering Role: The system engineer defines discrete lifecycle management activities for engineering disciplines and processes consistent with the FAA standard WBS, including human factors, configuration management, reliability, maintainability, and availability, among others. These elements are integrated into all other program planning activities as a basis for developing cost and schedule estimates and detailed planning for the solution.

F. Solicit and Evaluate Offers for Prime Contract(s)

The Contracting Officer issues a type of Screening Information Request called a Request for Offer after the Initial Investment Decision. The Request for Offer contains a Statement of Work, final functional and performance requirements, and contract terms and conditions for the selected alternative. Additionally, a contract-specific independent government cost estimate is prepared to assist in evaluating contract proposals.

A source selection team establishes an acquisition strategy and evaluation process, then evaluates technical proposals received from bidders for completeness, technical suitability, and compliance. The team also compares contractor offers to the government estimates of cost, benefits, schedules, and risks. If bidder estimates are deemed more realistic than FAA estimates, the team adjusts its risk management planning and proposed baselines. Note that a contract award is not made until after the Final Investment Decision which concludes the FIA phase.

Systems Engineering Role: The systems engineer assists the Contracting Officer in preparing the Request for Offer and may serve on the source selection team. The systems engineer uses input from key stakeholders and vendor proposals to refine requirements to lower cost or risk or increase performance and benefits while retaining critical performance needs. The systems engineer assists with development of the independent government cost estimate and with technical evaluation of vendor proposals.

G. Conduct Affordability Analysis

The investment analysis team forwards estimates of the life cycle costs to the Capital Investment Team. Capital Investment Team assesses the budget impact of the proposed program and its relative contribution to satisfying FAA goals against other investment options and make a funding determination. When a solution cannot be funded within the capital investment program baseline, the Capital Investment Team may propose offsets from lower priority programs. Preliminary budget impact assessments by the Capital Investment Team will shape subsequent deliberations of the Investment Analysis Team.

Systems Engineering Role: In a constrained resource environment, the systems engineer may be called upon to assist in evaluating the proposed investment's relative contribution to agency goals. Familiarity with the business case is instrumental to this task.

H. Finalize Business Case

The final business case demonstrates the value of implementing the proposed investment program and specifies the resources, budgets, schedules, and contract baseline(s) required to implement the solution. It is presented to the investment decision authority at the Final Investment

Decision. The final business case requires computation of the following economic measures: risk-adjusted cost, net present value, cost-benefit ratio, and payback period. Further guidance is available from the Investment Planning and Analysis organization.

Systems Engineering Role: The systems engineer thoroughly analyzes the selected alternative to ensure that performance specifications are consistent with final program requirements and that the implementation strategy conforms to agency standards. The systems engineer participates in sensitivity analyses that examine how variations in reliability, maintainability, availability, configuration management, human integration, manpower, documentation, interfaces, and specialty engineering affect solution cost, schedule, and risk. The systems engineer finalizes the enterprise architecture artifacts required for a final investment decision.

I. Develop In-Service Review Checklist

The In-Service Review Checklist is a tool for identifying, documenting, and resolving implementation and deployment issues. It enables detailed planning for solution implementation and lifecycle support, and determines readiness for the In-Service Decision that occurs at the end of the Solution Implementation phase.

Systems Engineering Role: The systems engineer participates in tailoring the In-Service Review Checklist to ensure that all key aspects of fielding a new capability and sustaining it over its service life are addressed in solution planning and funding documents. The system engineer also ensures that all engineering activities associated with developing, installing, testing, and transition from legacy assets to the new operational capability are included in implementation plans and budgets.

J. Verify and Validate Key Work Products

Verification and validation activities during FIA focus primarily on the final business case, final program requirements, ISPD, and Acquisition Program Baseline. This mitigates risk and ensures a solid foundation for the Final Investment Decision and the subsequent implementation of the best solution. The activity verifies that business case estimates were developed using sound practices and are both logical and realistic. Business case validation is detailed in the *Business Case Evaluation and Assessment Guide* provided by the Investment Planning and Analysis organization. Verification and validation for all other program documentation is conducted as described in the *AMS Lifecycle Verification and Validation Guidance Document* and Section 4.7: Verification and Validation.

Systems Engineering Role: The systems engineer leads verification and validation of final program requirements, and supports V&V for the other key work products if necessary. The systems engineer verifies that engineering costs and activities are adequately specified in program planning and budgeting documents.

K. Final Investment Decision

When the key investment analysis work products are sufficiently mature and fully validated and verified, the team prepares the final investment package and briefing materials for the Final Investment Decision. This is a major review and determines whether an investment opportunity is approved for funding and implementation. The investment decision authority approves, disapproves, or modifies the recommendations in the final investment package. If the authority disapproves the recommendations, it returns the investment package with specific instructions for further work or terminates the effort. If the authority accepts the recommendations, it then:

- Approves the investment program for implementation and delegates responsibility to the appropriate implementing service organization;
- Approves adjustments to FAA plans and budgets to reflect the investment decision.

Systems Engineering Role: The systems engineer is part of the team that prepares materials for the Final Investment Decision.

Table 5 summarizes the work products that are used and developed in the Final Investment Analysis phase. For more details on these artifacts and other aspects of this phase, use the references in Section 6.

Table 5: Final Investment Analysis Work Products

Product	Description	Supporting Processes
Final Program Requirements Document (fPRD)	Updates the Initial Program Requirements to provide a complete statement of functional and performance requirements. Final Program Requirements are tailored to the solution selected for implementation and form the basis for program assessment during Solution Implementation.	• Requirements Analysis
System Specifications	Derived from the program requirements, specifications provide low-level detail for functional and performance attributes of the selected solution.	• Requirements Analysis
Enterprise architecture products	The numerous "views" that describe various key aspects of the proposed solution. The ISEF document provides guidance on which products are needed.	• Architectural Design Synthesis • Interface Management • SE Information Management
Preliminary Hazard Analysis (PHA)	An initial effort in hazard analysis during the system design phase and the programming and requirements development phase for acquisition.	• System Safety Engineering
Final Business Case	An update of the business case from prior phases. The final business case demonstrates the value of implementing the proposed investment program and specifies the resources, budgets, schedules, and contract baseline(s) required to implement the solution. It is presented to the JRC at FID.	• Integrated Technical Management • SE Information Management
Risk for Solution	Risks associated with the proposed solution that threaten performance, cost, schedule, and benefit objectives are examined in greater depth during FIA.	• Risk, Issue, and Opportunity Management
Lifecycle Engineering (LCE) Cost for Solution	A calculation of the total lifecycle cost to design, develop, field, and operate the proposed solution.	• Integrated Technical Management • SE Information Management
Draft ISR checklist	A deployment planning tool to assist in identifying, documenting, and resolving deployment and implementation issues. An ISR template is available on the FAST site.	• Integrated Technical Management • SE Information Management
Final Implementation Strategy and Planning Document (ISPD)	Plans for utilizing organizational structure, control systems, and culture to develop and field the solution. Conveys the most critical, relevant, and meaningful information regarding the alternative selected for implementation.	• Integrated Technical Management • SE Information Management

Product	Description	Supporting Processes
Statement of Work (SOW)	The SOW is a detailed description of the specific services or tasks that a contractor is required to perform under a contract. The SOW is incorporated into a vendor contract.	• Functional Analysis • Decision Analysis • Integrated Technical Mgmt.
Work Breakdown Structure (WBS)	A WBS defines all work activities necessary to achieve the solution. It is the basis for project planning and estimations.	• Integrated Technical Management • SE Information Management
*Note: **Bolded** items are required as inputs to Solution Implementation.*		

2.2.5 Solution Implementation

Solution Implementation (SI) commences with the approval and funding of an investment program, and ends when a new service or capability is commissioned into operational use at all sites. The overarching goal of SI is to satisfy requirements documented in the final requirements document and achieve the benefit targets in the business case. To achieve this, the service organization must work with users, stakeholders, and vendors throughout SI to resolve issues as they arise.

The activities undertaken during SI vary widely and are tailored to the solution or capability being implemented. Essentially, this phase of the AMS management lifecycle consists of two distinct, yet often overlapping segments: Product Realization, and Deployment and Transition. The first segment transforms the work products of the approved Acquisition Program Baseline into products that comprise the designed solution – hardware, software, processes, etc. These products are then deployed to their intended destinations, installed, and transitioned into an operational status through a process that involves verification testing.

2.2.5.1 Product Realization

It is important to note that the FAA obtains solutions quite differently from an industrial "widget-maker". While both entities may apply many of the same SE principles during the conceptualization and initial development stages, the FAA almost always contracts with external vendors to develop and produce the assets that FAA acquires and deploys to satisfy its service needs. That is not to say that FAA is disengaged from the implementation and integration of its solutions. Systems engineers and subject matter experts perform critical oversight and advisory roles with contractors – to clarify requirements, assist with troubleshooting, support test activities, and manage schedules and budgets. The aspects of SI most relevant to systems engineering are described in detail below.

Figure 10 depicts the inputs, the basic phase activities, and the eventual outputs of the Product Realization sub-phase – it is referred to in other systems engineering manuals as "implementation and integration".

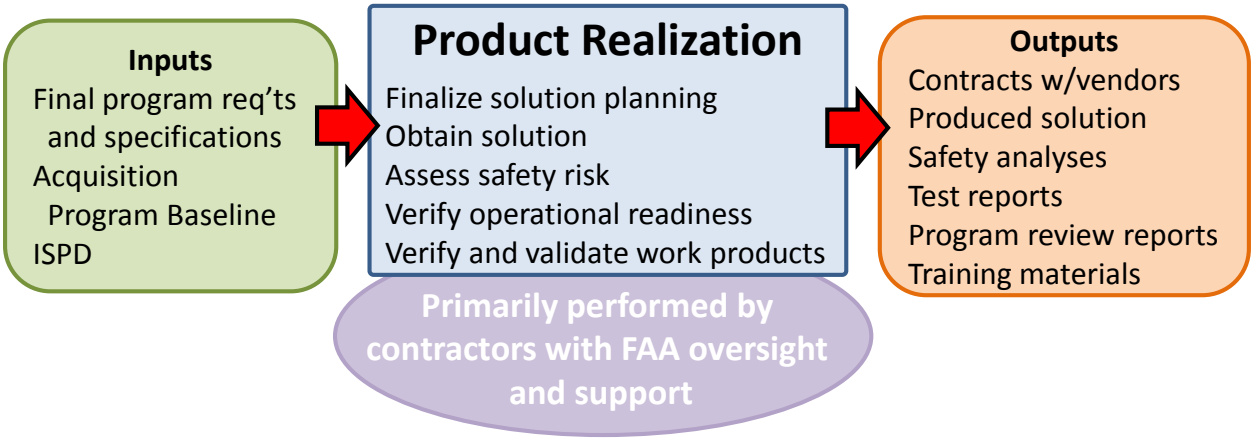


Figure 10: Product Realization Phase Diagram

Figure 11 provides a simple, notional depiction of some of the implementation and integration activities involved in Product Realization for a solution consisting of hardware and software. Note that not every solution element is created from scratch. Frequently, components of the final design are COTS products with previously demonstrated performance characteristics and quality controls. The use of COTS components in a design can simplify verification testing and reduce risk. The diagram also shows that a failed verification test will generally result in a rebuild or redesign of the element or assembly if a suitable mitigation is not available in the verification plans. The steps shown are typically performed by the vendor, although FAA systems engineers generally participate in or observe the verification tests.

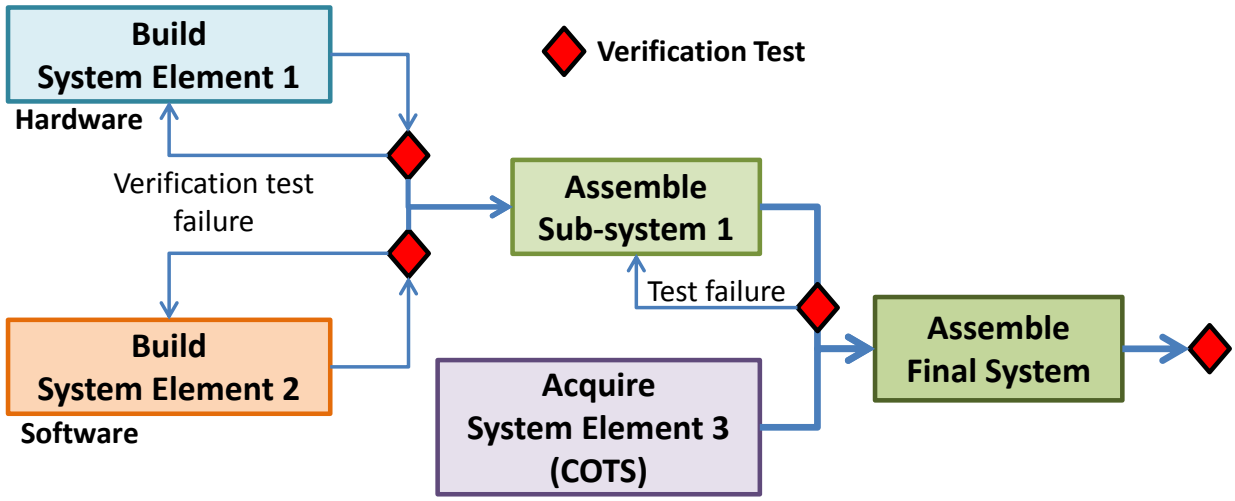


Figure 11: Notional Integration Process

Solution Implementation Activities

Product Realization consists of many activities which the systems engineer must either perform, support, or track. These activities are described below in more detail, and occur in roughly this order, although some overlap and iteration is typical.

A. Finalize Solution Planning

Key program stakeholders and vendor representatives join the implementation team to ensure that all implementation planning performed during FIA is complete and realistic. This may involve translating the overall strategy in the Implementation Strategy and Planning Document into discipline-specific planning for all aspects of program implementation and lifecycle support. Examples include a Test and Evaluation Master Plan, Systems Engineering Master Plan, Configuration Management Plan, and Logistics Support Plan. The plans that are required depend upon program complexity. It is crucial to clearly define the role of each government organization and contractor in program execution. For example, if new systems are to be installed or existing facilities modified, service organization planners must work with service-area offices so people and resources will be available when the work must be done.

Systems Engineering Role: The systems engineer ensures that technical planning is sufficient and addresses all systems engineering disciplines necessary for obtaining the solution. The systems engineer has the following duties:

- Ensure that work is performed in accordance with the vendor's Systems Engineering Management Plan
- Participate in post-award conferences to ensure a mutual understanding of requirements
- Establish technical measures to monitor and control the program
- Baseline technical risks and develop mitigation plans
- Establish entry and exit criteria for technical reviews
- Identify independent subject matter experts for participation in technical reviews
- Assist in developing Integrated Master Schedule tasks and resulting technical products
- Prepare for the Integrated Baseline Review

B. *Obtain Solution*

This activity includes all tasks necessary to develop the solution to the point where it is ready to be verified for operational use and deployed to an operational environment. On the FAA side, obtaining the solution typically includes such activities as contract award, contract administration, program management, resource management, risk management, systems engineering, logistics support analysis, test and evaluation, and site acquisition and adaptation. This may also involve developing operational procedures and training materials; ensuring physical, personnel, and information security; modifying the physical infrastructure; and coordinating collateral action by the aviation industry. On the vendor side, this activity is substantial, as it includes the detailed design and fabrication efforts required to produce, assemble, and integrate the solution. See Figure 11 for a notional illustration of this process.

Verification testing is an integral part of obtaining the solution. As solution elements are completed – generally by the solution vendor – they must meet the criteria set forth in the Verification Plan before further assembly can occur. Testing ensures conformance with performance, design, and interface requirements at each level of assembly. Most NAS solutions are actually part of a "system of systems", in which interfaces are especially critical. This activity culminates with verification and acceptance testing to demonstrate the end-to-end operation of the designed solution.

Systems Engineering Role: A systems engineer frequently serves as the technical subject matter expert for the program. This role entails participating in user interviews, rapid prototyping, demonstrations, or any other activity that shows the requirements to be well understood, consistent, and appropriate before starting detailed design. The systems engineer oversees and monitors program design reviews such as the System Design Review, Preliminary Design Review, and Critical Design Review. The system engineer also reviews and approves technical contract deliverables.

The systems engineer also proactively considers technology integration, business integration, and user integration concerns. Technology integration can be defined as the melding of various technologies into a functional whole. Business integration refers to issues that arise when multiple organizations work together to complete a system. It can also refer to the integration of business processes. User integration addresses human factors issues and focuses on the system from an end-user point of view.

C. *Assess Safety Risk*

Safety specialists perform multiple analyses during Solution Implementation:

- Subsystem Hazard Assessment (SSHA) – examines each subsystem or component to identify and assess hazards
- System Hazard Assessment (SHA) – analyzes a system's interfaces with other systems, and between its subsystems
- Operating and Support Hazard Assessment (O&SHA) – primarily identifies and evaluates those hazards associated with interactions between humans and equipment
- System Safety Assessment Report (SSAR) – an overall assessment of the risk in the system

Systems Engineering Role: Depending on experience and the size and complexity of the initiative, systems engineering personnel may perform or support the safety assessment and produce the resulting documentation.

D. *Verify Operational Readiness*

This activity includes all tasks necessary to install the solution at a designated field test site and evaluate it thoroughly to ensure operational readiness. Operational readiness encompasses operational effectiveness and operational suitability. Operational effectiveness measures how well the solution satisfies service needs and operational requirements. Operational suitability

measures how well a product is integrated within its intended environment and prepared for field use, considering such factors as compatibility, reliability, human factors performance, maintenance and logistics support, safety, and training. Some locations where the realized solution may be installed for readiness testing include the FAA Academy, FAA Logistics Center, or William J. Hughes Technical Center. Before a solution can be placed into operational use, it requires an officially declared operational readiness date.

Systems Engineering Role: The systems engineer ensures activities and resources for the operational readiness evaluation are sufficient to accomplish its objectives. Based on the contractually required activities, the systems engineer ensures that the prime contractor demonstrates conformance to contract specifications, thereby resulting in government acceptance.

E. Verify and Validate Key Work Products

Throughout the entire SI phase, the program team validates and verifies key work products used in SI, including during Deployment and Transition activities. Key work products may include the vendor contract, architectural design documents, interface documentation, and hardware/software product specifications. Verification activity supports contract award, preliminary and final design reviews, product demonstration and production decisions, solution acceptance, and the In-service Decision that concludes SI. For further guidance, see Section 4.7: Verification and Validation.

Systems Engineering Role: The systems engineer assists in verifying and validating key work products during Solution Implementation.

Table 6 summarizes the work products that are developed and used in the Product Realization segment of the Solution Implementation phase. For more details on these artifacts and other aspects of this phase, use the references in Section 6.

Table 6: Product Realization Work Products

Product	Description	Supporting Processes
Agreement on system specifications (Note: may include Interface Control Documents, Refined System Specification, System/Segment Specification)	The successful outcome of a System Requirements Review (SRR). The SRR forms the basis for determining (1) whether system requirements are consistent, achievable, and complete, and (2) whether the government and contractor have a clear and mutual understanding of them. While the contractor conducts this review, the government takes an active part by clearly defining expectations and standards before the review and by participating actively in the event.	• Functional Analysis • Requirements Analysis • Decision Analysis • Specialty Engineering
Approval to begin detailed design	The successful outcome of a formal review of initial design concepts and documentation to confirm the preliminary design meets requirements.	• Functional Analysis • Decision Analysis
Sub-system Hazard Analysis (SSHA)	Performed if a system under development contains subsystems or components that, when integrated, function together in a system. The Contractor shall examine each subsystem or component and identify hazards associated with normal or abnormal operations and determine how operation or failure of components or any other anomaly adversely affects the overall safety of the system.	• System Safety Engineering

Product	Description	Supporting Processes
System Hazard Analysis (SHA)	A safety risk assessment of a system that analyzes the interfaces of a system with other systems, as well as the interfaces between the subsystems of the system under study. The contractor-performed SSHA serves as input to the SHA.	• System Safety Engineering
Risks	The risks associated with developing the propose solution.	• Risk, Issue, and Opportunity Management
Request for Action (RFA) (When applicable)	In the event that some aspect of the design does not meet requirements, a request to take action to correct the problem is made.	• Requirements Analysis • Decision Analysis
Production Decision	A successful outcome of the Critical Design Review (CDR) which evaluates the completeness of the design, its interfaces, and suitability to start initial manufacturing or development. Note: Could be part of a Decision Analysis Report (DAR)	• Decision Analysis • Specialty Engineering
Test Readiness Review (TRR) products	The contractor conducts a System Test Readiness Review (TRR) using a process similar to that in MIL-STD-1521B to provide documented proof that all requirements necessary to start Formal Qualification Testing (FQT) have been met. Includes Final System Test Procedures and Agreement to proceed with Formal Qualification Testing.	SE supports with information from: • Decision Analysis • Integrated Technical Management
Verified and validated solution products	Performance of Formal Qualification Testing (FQT) shows that the proposed solution can perform all required design functions and satisfy final requirements.	• Integrated Technical Management • Verification & Validation • Specialty Engineering
Functional Configuration Audit (FCA) Report	Verifies that the system and all subsystems can perform all of their required design functions in accordance with their functional and allocated configuration baselines. This can include the gap of required versus verified performance.	• Configuration Management
Verified Program Baseline	The output from a Physical Configuration Audit (PCA). The service team conducts a PCA after all test programs are completed, as close to production of the first unit as possible. The PCA examines the "as-built" product against its design documentation to establish the product baseline. The PCA includes a detailed audit of engineering drawings, specifications, technical data, and tests used in the production of HWCIs, and design documentation, code listings, and manuals for CSCIs. The review includes an audit of released engineering documentation and quality control records to ensure the "as-built" and "as-coded" configuration is reflected by this documentation.	• Configuration Management
Baselines and Updated Baselines	Baselines are established during the CM process and any changes to these baselines are released in the form of updated baselines.	• Configuration Management

2.2.5.2 Deployment and Transition

Activities performed during Product Realization ensure that the solution is ready to be deployed to the field. The product or system might have worked perfectly at the vendor's facility, but it must also satisfy the program requirements in an operational environment. Deployment and Transition (D&T) activities ensure that the solution is successfully deployed and is transitioned into an operational status.

The D&T sub-phase encompasses a variety of planning, assessment, and preparation activities which are essential to fielding a solution; these activities determine solution readiness and ensure the integrity of the operational system. Trouble-free deployment and transition requires thorough planning early in the lifecycle and collaborative efforts between the service organization, contracted vendors, and personnel from the relevant regions and facilities.

When a solution is to be fielded at multiple sites, deployment can sometimes start while the solution is still being produced. The underlying objective is to ensure that all operational aspects have been accounted for prior to transitioning operations to the new product, capability, or functionality. Similarly, transition activities may sometimes commence before the solution has been deployed to every site. The objective of transition is to facilitate a seamless operational switchover from the legacy asset or system to the newly installed solution. Minimizing or avoiding risk is paramount, depending on the type of operations impacted by the new solution.

Section 5.2: Life Cycle Engineering discusses the development of a Lifecycle Plan, which documents how to transition operations and maintenance from an operational asset to its replacement, including preparations, installation, testing, dual operations, training, and disposal issues. Ultimately, the transition process transfers custody of the system and responsibility for system support from a developmental entity to an operational and support organization.

Figure 12 summarizes the essential inputs, activities, and outputs of Deployment and Transition.

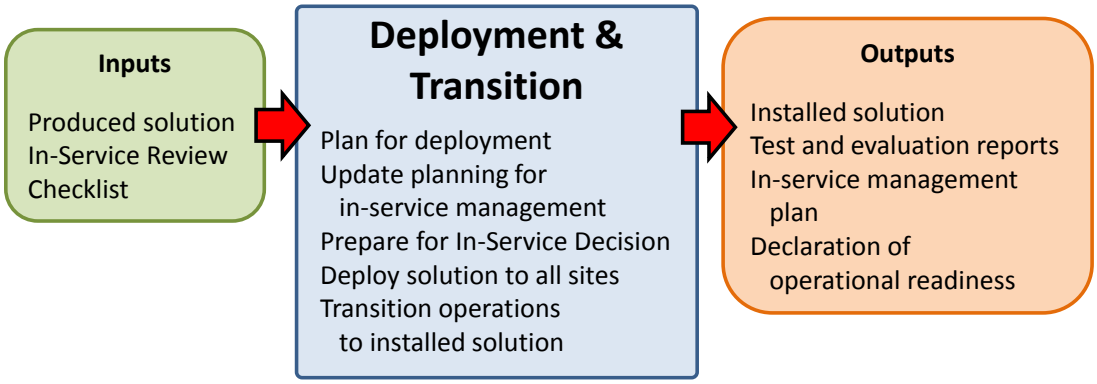


Figure 12: Deployment and Transition Phase Diagram

Activity Descriptions

Deployment consists of many activities which the systems engineer must either perform, support, and track. These activities are described below in more detail, and occur in roughly this order, although a fair amount of overlap and iteration is frequently necessary.

A. Plan for Deployment

Deployment planning prepares for and assesses the readiness of a solution to be implemented and is also part of the Lifecycle Plan. Deployment planning is part of a continuous In-Service Review process that begins early in the lifecycle management process, usually during development of requirements in the CRD phase. Deployment planning involves coordination

among and participation by many critical functional disciplines. Tradeoffs among cost, schedule, performance, and benefits relative to these functional disciplines must also include the impact of deployment and transition considerations. Deployment planning tools – such as the In-Service Review checklist – assist in identifying, documenting, and resolving deployment and transition issues.

Deployment planning techniques include: customizing generic tools; integrating checklist issues with other emerging issues, such as verification test problems; developing action plans to resolve checklists; and documenting issue resolution and mitigation results. Deployment planning is documented in the contractor's Statement of Work, among other places. The results of deployment planning and issue resolution are briefed periodically at acquisition reviews, presented at the In-Service Decision (ISD) meeting, summarized in an ISD memorandum, and audited during the post-ISD follow-up and monitoring activities.

Systems Engineering Role: The systems engineer ensures that technical planning is completed and that sufficient engineering resources are identified for deploying the solution at all scheduled facilities. The systems engineer also verifies that the deployment planning package is compatible with ongoing operations. The systems engineer must have an in-depth understanding of the resolution of integration issues involved with legacy systems at the sites.

B. Update Planning for In-Service Management

This activity establishes how the solution will be sustained and managed throughout its full service lifecycle. It focuses on in-service support, but includes post-implementation reviews and periodic evaluation of operational assets. These measure performance and supportability trends and include service-level reviews, product-sustainment strategy, service-life extension, and eventual removal from service, including site restoration.

Systems Engineering Role: The systems engineer ensures that technical planning for sustaining the solution through its planned service life is sufficient, feasible and that it addresses all necessary systems engineering disciplines. The systems engineer reviews and updates lifecycle technical planning documents relating to preventive and corrective maintenance, supply chain management, second-level maintenance, and hardware and software depot support. The systems engineer also verifies that the planned lifecycle support and management structure is being realized via maintenance resource requirements, spare/repair parts, test and support equipment, personnel resources, training resource requirements, environment, safety, health. Finally, systems engineering must help evaluate plans for decommissioning the replaced operational assets while considering environmental laws, regulations, and directives.

C. In-Service Decision

In order to proceed to the In-Service Decision, the service organization charged with deploying the solution must first complete the following activities: resolve all support issues identified by the operating service organization and integrated logistics management team; complete management actions arising from the In-Service Review checklist and the independent operational analysis report (if applicable); resolve stakeholder issues; develop the In-Service Decision briefing and action plan; and obtain the concurrence of key stakeholders. If the In-Service Decision authority determines that the solution and its support package are sufficient for deployment into the operational environment, it approves the plans and the subsequent deployment and transition activities commence.

Systems Engineering Role: The systems engineer supports the program manager technically and programmatically in all aspects of obtaining a favorable decision from the In-Service Decision authority.

D. Deploy Solution to All Sites

The solution will have been deployed to at least one operational site before an in service decision is made. Deploy Solution includes all activities necessary to install the solution at each site and bring it into operational use. This may involve transportation and delivery of equipment to each site, installation and checkout, contractor acceptance and inspection, integration with other

assets, field familiarization, declaration of initial operational capability, joint acceptance and inspection, dual operations, declaration of operational readiness, and removal and disposal of obsolete equipment. The transition from solution implementation to in-service management extends over time, occurring at each site upon declaration of operational readiness or commissioning.

Systems Engineering Role: The systems engineer ensures all activities necessary to transport, deliver, receive, process, assemble, install, checkout, train, operate, house, store, or field the solution to achieve full operational capability are completed and operating efficiently.

E. Plan and Perform the Operational Transition

Operational transition is typically a smooth continuation of deployment activities and includes consideration of the following tasks: operator training, logistics support, delivery strategy, issue resolution, cut-over plan, and installation procedures. Some specific tasks that are typically necessary to complete the transition:

- Prepare site for new solution
- Install, integrate, and verify the new solution
- Train users and maintenance personnel
- Conduct Independent Operational Test and Evaluation
- Conduct dual operations at site
- Implement cut-over plan
- Document post-implementation issues
- Commission site into operational service

Systems Engineering Role: The systems engineer ensures that technical planning is completed and that sufficient engineering resources are identified for transition activities at all scheduled sites. Depending on the level of risk, the systems engineer may require a contingency plan for any anomalies. The systems engineer ensures that all transition tasks are performed in accordance with approved FAA guidance and good systems engineering practices. The systems engineer provides oversight and quality assurance to these activities but can also be a key participant in some transition tasks.

Table 7 summarizes the work products developed and used in the Deployment and Transition segment of the Solution Implementation phase. For more details on these artifacts and other aspects of this phase, use the references in Section 6.

Table 7: Deployment and Transition Work Products

Product	Short Description	Supporting Processes
Baseline Changes	Baseline changes are provided to all CM users whenever a potential change or update is pending that could impact their work product	• Configuration Management
Configuration Status Accounting Reports (CSAR)	Configuration status accounting reports (CSAR) provide the current status of CI configuration items or work products. CSARs can be generated electronically and are provided on demand or at scheduled intervals by the supporting CM process.	• Configuration Management
Operating & Support Hazard Analysis (O&SHA)	Performed by the Contractor primarily to identify and evaluate hazards associated with the interactions between humans and equipment/systems. These interactions include all operations conducted throughout the lifecycle of the solution.	• System Safety Engineering
Operational Baseline	The operational baseline is the approved technical documentation representing installed operational hardware and software. This represents a product baseline adapted to local conditions. Operational baselines comprise the technical documentation that initially describes a delivered solution.	• Configuration Management
System Safety Assessment Report (SSAR)	A report to provide management an overall assessment of the risk associated with the solution prior to fielding, but also must be employed, prior to operation of the solution. This is accomplished by providing summaries of the analyses and testing results.	• System Safety Engineering
System Safety Program Plan (SSPP)	The Safety office will review the prime vendor's System Safety Program Plan (SSPP) and if it meets all requirements, they will accept the plan.	• System Safety Engineering
Operator and User Manuals	Manuals that prescribe the proper use of the installed equipment or software.	• Integrated Technical Planning • SE Information Management

2.2.6 In-Service Management

Activity during in-service management supports execution of the FAA mission of providing air traffic control and other services. This entails operating, maintaining, securing, and sustaining systems, products, services, and facilities in real-time to provide the level of service required by users and customers. It also entails periodic monitoring and evaluation of fielded products and services, and feedback of performance data into service and investment analysis as the basis for revalidating the need to sustain deployed assets or taking other action to improve service delivery.

In-service management planning documents focus on actions and activities that support continued operation and maintenance of deployed assets. The documents clearly define in-service management activities such as configuration management, preventive and corrective maintenance, training, infrastructure support and logistics support, along with planned activities to support post-implementation reviews and operational analyses. Changes in the NAS operating environment, changes to requirements or interfacing equipment, safety and security issues, long term or cyclical development issues, loss of replenishment part suppliers, and significant NAS Change Proposal (NCP) reviews may involve system engineering support.

When a fielded capability is projected to be unable to satisfy service demand or when another solution offers improved safety, lower cost, or higher performance, the service organization initiates action to enter the service analysis process leading to a new investment decision. The key is to look far enough into the future so there is enough time to approve and implement a new solution or technical refresh before the existing capability fails or becomes obsolete. Systems engineers may be called upon to produce planning artifacts – legacy specifications, business cases, and other AMS documentation – in support of replacement planning long before the end of service life.

Figure 13 summarizes the essential inputs, activities, and outputs of In-Service Management.

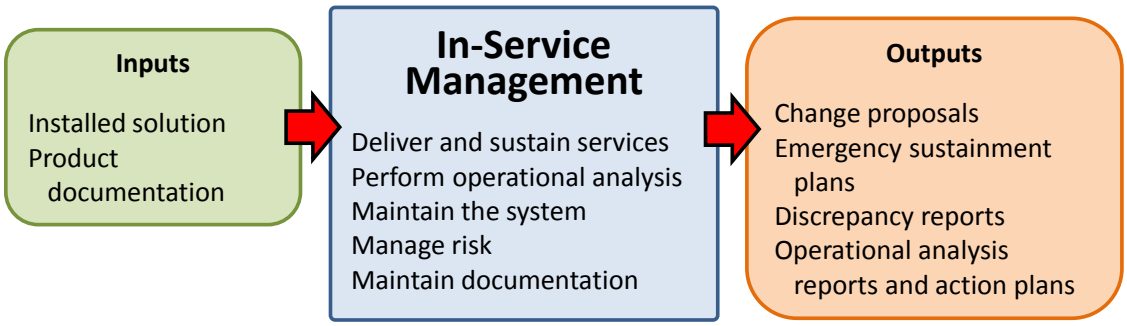


Figure 13: In-Service Management Phase Diagram

Activity Descriptions

In-Service Management consists of several activities which the systems engineer must either perform or support over the lifecycle of the installed solution. These activities are described below in more detail.

A. Deliver Services

Service delivery is per the infrastructure, procedures, personnel, and other assets as planned, assigned, and funded in prior phases of development.

Systems Engineering Role: The systems engineer typically is not involved with normal FAA operations. The systems engineer may play a role in the event of contingency operations.

B. Sustain Services

Management and engineering efforts throughout in-service management sustain and improve service delivery, correct deviations from cost and performance standards, and improve quality.

These efforts include hardware and software modifications to solve latent or discovered technical problems, process changes to improve performance, planned block upgrades and product improvements, and sustainment actions that lower operating costs. It involves managing personnel, information systems, budget, logistics support, spare parts, technical resources, and other assigned assets. Management techniques include fiscal and workforce planning, contract award and administration, fiscal and program control, and process management to achieve cost, performance, and benefit objectives. All modifications to fielded assets must be in accordance with the enterprise architecture. If a planned modification requires a change to the architecture, appropriate amendments and products must be developed and approved.

Systems Engineering Role: The systems engineer analyzes, recommends, and implements proposed software/hardware and support modifications that enhance the solution by accomplishing one or more of the following: address identified issues, process changes to improve performance, upgrade software or hardware, and perform sustainment actions that lower operating costs. The systems engineer contributes to developing emergency sustainment plans and service life extension plans.

C. Perform Operational Analysis

Periodic operational evaluation of fielded assets helps determine whether performance and customer expectations are being achieved. This type of evaluation continues throughout in-service management helping identify performance shortfalls, cost-of-ownership trends, and adverse support trends. The information gathered helps evaluate and solve systemic problems and forms the basis of whether to continue to sustain existing assets or to recommend new investments or upgrades.

In-Service decision making needs to take two factors into account: (1) assessing the timing for technology insertion or capability replacement, and (2) determining whether modifications or improvements are feasible within approved sustainment baseline funding. If an engineering change to the solution within the sustainment funding is unable to be supported, then the shortfall is addressed via the standard AMS lifecycle phases. If the effort to modify and/or optimize performance is within the scope of sustaining funds, then the various SE elements are employed as in the Solution Implementation phase but on a lesser scale. The specific SE process application and associated level of effort depend on the scope of the upgrade.

Systems Engineering Role: The systems engineer evaluates current and past operational data of the fielded asset to determine if expected performance and customer expectations have been attained. The role also includes preparing any needed hardware discrepancy reports.

D. Maintain the Solution

Modifications to fielded assets must be accompanied by associated support infrastructure changes such as training, documentation, spare parts, and relevant engineering support. This includes training for personnel who directly operate, maintain, and/or support the asset.

Systems Engineering Role: The systems engineer maintains the numerous components tied to a modification of fielded assets. This would include, for example, procedures, training, and support for a hardware or software modification.

E. Manage Risk

Risk needs to be managed throughout in-service management. The risk planning accomplished earlier in the lifecycle should be periodically reviewed to ensure that it still is adequate. When necessary, risk plans are used to mitigate risk.

Systems Engineering Role: The systems engineer supplies the engineering perspective to all risk issues. This includes recommendations to reduce potential risks by changing procedures or providing training.

F. Maintain Product or Service Documentation

To ensure configuration control and FAA reporting requirements, the documentation for the product and service needs to be accurately maintained.

Systems Engineering Role: The systems engineer provides the information that needs documentation and provides an engineering perspective to the operational personnel involved with preparing the documents. A key concern to the systems engineer is maintaining up-to-date configuration records.

Table 8 summarizes the work products developed and used in the In-Service Management phase. For more details on these artifacts and other aspects of this phase, use the references in Section 6.

Table 8: In-Service Management Work Products

Product	Description	Supporting Processes
Continued Investment Recommendation	An output of In-Service Performance Review (ISPR) used to characterize In-Service technical and operational health of the deployed asset by providing an assessment of risk, readiness, technical status, and trends in a measurable form that will substantiate In-Service support and funding.	The SE can support the program using aspects of • Integrated Technical Management • SE Management
Emergency Sustainment Plans	Plans for the continuity of operations in the event of an emergency that might impact some aspect of normal operations. Planning would include sustainment of utilities, buildings, grounds, structures, roads, telecommunications, and security.	• Risk, Issue, & Opportunity Management • Integrated Technical Management
Hardware Discrepancy Reports (When needed)	The service team test lead monitors, tracks, and assesses asset performance on a continuing basis throughout in-service management. When a hardware discrepancy is discovered, a report is issued.	• Integrated Technical Management • Verification and Validation
NAS Change Proposal (NCP) (When needed)	The formal method to request a change to the NAS. This usually occurs when a system or part of a system needs to be modified from its final specifications due to new discoveries while operating the system.	• Configuration Management

This page intentionally left blank.

3 Systems Engineering Processes

This section introduces and details the various systems engineering processes that must be performed to progress a concept into a solution. This occurs within the framework of the FAA acquisition management life cycle described in Section 2.

3.1 Operational Concept Development

An operational concept is essentially a proposal outlining how FAA resources—personnel, technology, and procedures—work together to satisfy a set of well-defined goals or needs. Several elements of FAA policy, planning, and guidance provide the foundation and framework for development efforts—the NAS Enterprise Architecture, the Acquisition Management System, NextGen Implementation Plan, Infrastructure Roadmaps, as well as external research in industry and academia.Operational Concept Development encompasses two key activities—Concept Development and Concept Validation. These activities are performed in an incremental and iterative manner to arrive at the point where feasible solutions may be analyzed for FAA investment.

Concept Development is a progression through a sequence of activities that includes defining and analyzing solutions to satisfy the operational needs of stakeholders, systematically investigating their feasibility, and ultimately developing an integrated concept evaluation environment. Concept development commences by describing an operational concept in detail sufficient to evaluate benefit mechanisms, identify research issues, and develop preliminary requirements. As research is performed, this detail is documented in a Concept of Operations (ConOps) and other documents.

Concept Validation is a process that underlies concept development and ensures that the correct operational solutions are being developed to meet the defined service needs. There is a close relationship between concept development and validation, as the latter helps guide the former. Concept validation ensures that all operational aspects are addressed and helps quantify and qualify the expected benefits of a proposed solution. Validation activities are iteratively performed throughout concept development to reduce implementation risk. Results from these activities are released to stakeholders and coordinated with the user community to determine whether changes to the concept and further validation activities are necessary. Models and prototypes are examples of the products that may be developed to validate maturing concepts.

An operational concept may be developed at various levels. For example, a Service-level concept is likely to impact or be part of the overall NAS Concept of Operations. At the other end of the spectrum is a Solution-level concept which describes a single technical solution or operational improvement. It is crucial that lower-level concepts are consistent with the relevant higher-level concepts. Validation helps to ensure this compatibility and linkage.

The end result of Operational Concept Development is a fully vetted ConOps document and preliminary analyses of service shortfalls, concept costs, benefits, and associated risks. The ConOps document quantitatively and qualitatively describes the needs of the stakeholders and depicts the envisioned solution from the user's point of view. As the ConOps is developed and reviewed, stakeholder needs are refined into operational requirements, as detailed in Section 3.3, Requirements Analysis. Operational Concept Development is generally performed during the Service Analysis and Strategic Planning AMS life cycle phase. In particular, the supporting activity known as Research for Service Analysis (RSA) is focused on concept development work. That section provides a high-level view of RSA, while the material below contains a more detailed description of the individual efforts and work products required.

Figure 14 summarizes the key inputs, activities, and outputs of the Operational Concept Development process.

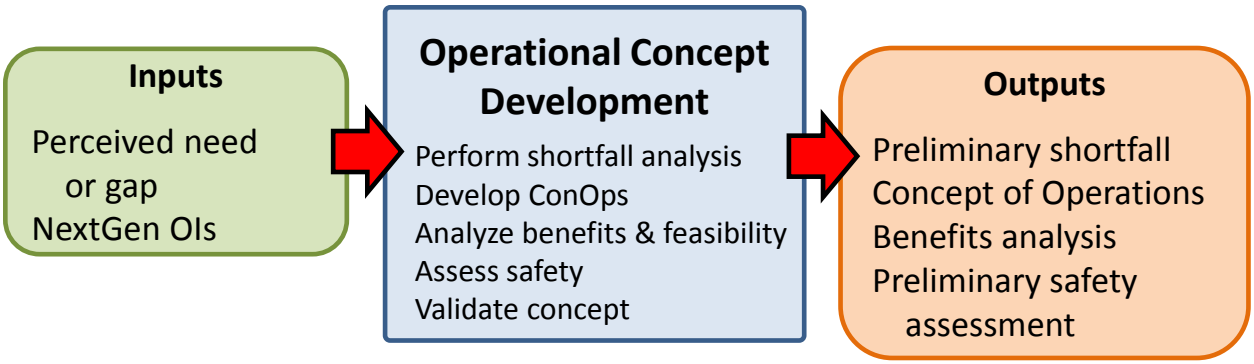


Figure 14: Overview of Operational Concept Development

3.1.1 Inputs

Inputs to Operational Concept Development include the following:

- Perceived need or gap
- NextGen Operational Improvements (OI)

3.1.2 Process Components

Operational Concept Development is comprised of the following activities:

- Perform shortfall analysis
- Develop Concept of Operations (ConOps) document
- Analyze concept benefits and feasibility
- Assess concept safety
- Validate concept
- Identify research issues (e.g., human factors)

These activities are not necessarily performed in the order listed, as concept development and validation is inherently iterative in nature.

Perform Shortfall Analysis

Service shortfalls are identified along with new concepts for improving service delivery. A shortfall is the difference between future service needs and current capability. When a shortfall impacts the NAS, it enters the NAS ConOps change development and decomposition process to determine how it fits within the NAS. See AMS policy, section 2.3.1 for further guidance on the NAS ConOps change process. Key activities contributing to the shortfall analysis include the following:

- **Gather information on the service environment**. Opportunities for improving service delivery and aviation service need forecasts form a basis for determining and prioritizing service needs and shortfalls. Input and feedback from customers and users form a part of this informational foundation.
- **Analyze service shortfalls and concepts**. Identify business, technology, organizational, process, and personnel issues that affect service outcomes and the related assumptions, risks, and dependencies.

- **Assess FAA Strategic and Performance Goals**. Shortfalls should reflect the gap between current services and the fulfillment of FAA strategic and performance goals. The shortfall must be shown to have sufficient merit to warrant inclusion in agency strategic planning documents.
- **Prepare the Preliminary Shortfall Analysis**. The shortfalls are analyzed as a foundation for understanding the problem's urgency and impacts. At this stage, the shortfall is expressed as levels of service improvement, not by specific performance values.

The Preliminary Shortfall Analysis is used to determine whether the service shortfall or new idea is addressed in the ConOps. Shortfalls are documented in the ConOps as Operational Improvements (OI) and Operational Sustainments (OS), that is, initiatives necessary to improve or sustain existing operations. New shortfalls that are within the scope of the ConOps proceed by decomposition into operational requirements and investment initiatives after determining whether they should be incorporated into new or existing operational capability development work. For shortfalls not in the ConOps, it must be determined what development or validation activities are needed.

Develop Concept of Operations Document

A key work product of Operational Concept Development is the ConOps. It is the primary repository for documenting the assumptions, constraints, and operational environment of the concept. The ConOps clearly states the concept's operational and functional characteristics within the intended operational environment. The first draft of the ConOps should include:

- Traceability to relevant Operational Improvements
- Clear definition of the problem
- List of all relevant assumptions and constraints, including those based on interdependent agency initiatives (e.g., NextGen concepts with overlapping functionality)
- Description of the concept's operational environment
- Summary of the expected benefits

These concept-level requirements are very preliminary operational requirements which will continue to be refined during Requirements Analysis.

Analyze Concept Benefits and Feasibility

The concept should provide or contribute to improvements in FAA Air Traffic Operations as envisioned by NextGen. The NextGen Implementation Plan describes the benefits of the Operational Improvements (OI) to the aviation community. To the extent that the concept is supporting a NextGen OI, the benefit can be listed.

There can be technical, political, and cultural factors involved with concepts that involve changes in procedures, staffing, or facility location. This SEM will only address the technical feasibility of the concept. Evaluating concept feasibility includes concept integration, evolution, and scalability. Representative activities include simulations, prototyping, and field demonstration.

Assess Concept Safety

A preliminary Safety Impact Assessment (SIA) is developed to identify potential safety benefits and hazards of the proposed concept. This can be done in a variety of ways but is often approached by comparing proposed changes in the operating environment in a side-by-side analysis or a task analysis.

Further safety-related activities focus on identifying and characterizing specific hazards based on the proposed operational implementation of the concept. These efforts should focus on supporting Operational Safety Assessment (OSA) as part of what will become the concept transitional package. As the process nears completion, the Operational Service and Environment Description (OSED) and Operational Hazard Assessment (OHA) portions of the OSA should be substantially drafted.

Validate Concept

As noted earlier, Concept Development and Concept Validation are two separate, often parallel, processes. These processes help to systematically explore how a proposed concept will impact the NAS. Validation -- ensuring that a concept is an appropriate solution to meet the defined service needs - is a critical and continuing process. Not all methods of validation listed are appropriate for all concepts, so care must be taken when selecting the methods to use. Generally, all of the validation activities listed here require some form of input from user groups in the form of subject-matter experts or system users.

The following is a list of commonly used techniques in the concept validation process:

- Paper Studies
- Knowledge Elicitation
- Cognitive Walkthroughs
- Modeling
- Human Performance Studies
- Fast-time Simulation Studies
- Real-time Human-in-the-Loop (HITL) Simulations
- Rapid Prototyping
- Field Demonstration

For more detail on any of these analysis and validation activities, refer to the *Concept Development and Validation Guidelines* document. In addition, Section 3.5, Cross-cutting Technical Methods describes the use of models, simulations, and prototypes in systems engineering.

3.1.3 Outputs

Operational Concept Development is the process that describes and evaluates a proposed capability, technology, or procedure (collectively referred to as a concept) for Investment Analysis. The focus of concept development is to establish and refine operational needs, attributes, initial performance parameters, and constraints. These factors are translated into preliminary operational requirements, which may include early performance parameter objectives and thresholds, affordability constraints, and technical constraints. Typically the final outputs of this process are the following:

- Preliminary shortfall analysis
- A fully vetted ConOps document
- Benefits analysis - a preliminary analysis of concept costs and expected benefits
- Preliminary safety assessment
- Research issues requiring more investigation

3.1.4 Concept Maturity Levels

The Concept Maturity Level (CML) system is a measure used to assess the maturity of an evolving concept. The primary purpose of using concept maturity levels is to provide a common understanding of a concept's developmental status. Specifically, a CML designation is used to determine funding allocations, align NextGen research priorities, and track concept progress.

Figure 15 provides an overview of CML progression during the Operational Concept Development process. The FAA *Concept Development and Validation Guidelines* provide much more detail into the CML paradigm, and the levels are summarized below.

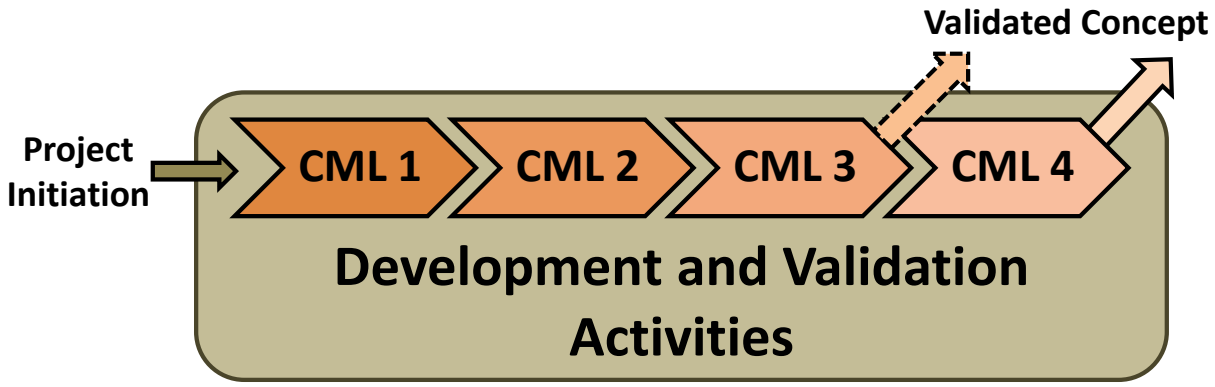


Figure 15: Concept Maturity Levels

In CML 1, multiple solutions to a service need may be explored. By the end of CML 1, a specific concept has been selected for further development and validation. CML 2 occurs when a draft ConOps is developed and initial concept-level requirements are identified. CML 3 typically involves formulating detailed operational scenarios and an integrated concept prototype for advanced concept validation. Examples of an integrated prototype include a human-in-the-loop (HITL) simulation or field demonstration. If transition from research to program initiation does not occur after CML 3, then CML 4 represents the final phase of concept refinement and validation. By the end of this level, the concept has been explored, analyzed and sufficiently evaluated for operational and technical feasibility to support the subsequent investment analysis process.

Additional Information

For sources of information used to generate content throughout this section, see References.

To learn more about the topics in this section, see Additional Tools and Reading Recommendations.

3.2 **Functional Analysis**

The Functional Analysis process examines the functions, sub-functions and interfaces that accomplish the solution's operation or mission. While the Operational Concept defines the *way a solution will be used*, the functional analysis process focuses on *what* the solution does, not *how* it does it. The Functional Analysis process provides two key systems engineering benefits:

- Avoiding single-point solutions
- Describing the behaviors that lead to requirements and physical architectures

A *function* is a characteristic action or activity that has to be performed in order to achieve a desired system objective (or stakeholder need). A *function name* is stated in the form of an action verb followed by a noun or noun phrase; it is an action that describes the desired system behavior. Examples of common functions include "read book," "eat food," and "go to store." A function occurs within the system environment and is accomplished by one or more system elements composed of equipment (hardware, software, and firmware), people, and procedures to achieve system operations. Each function required to meet the operational needs of a system is identified, defined, and organized into a functional architecture. In Functional Analysis, because a function may be accomplished by more than one system element, functions are unable to be allocated. Rather, functions are used to develop requirements, which are then allocated to solutions in the form of a physical architecture. Using the Functional Analysis process significantly improves design, innovation, requirements development and integration.

The purpose of the Functional Analysis process is to transform the stakeholder needed capabilities, described in the ConOps document into a functional view of a required system (regardless of complexity) that could deliver those capabilities. The first functions to identify come from the need(s), which is then decomposed into lower levels of needed functionality (Figure 16 illustrates the Functional Analysis process flow). This process builds a representation of a future system or potential system of systems that will meet stakeholder expectations and that as far as constraints permit, does not imply any specific implementation. The functions developed in this process are used to develop a complete set of system-level requirements that specify what characteristics the system is to possess and the performance of those characteristics in order to satisfy stakeholder expectations. The FAA preference is to translate a function into a Primitive Requirement Statement (PRS), then transition the PRS into a mature requirement, and finally allocate the mature requirements to physical architecture entities. Functional Analysis is critical in developing a complete, high-quality set of requirements.

The following are results of the successful implementation of the Functional Analysis process:

- The required functions for a solution are described, recognized and specified. The required inputs and outputs to support and attain system function are defined.
- Constraints that will affect the design of a system and the means to realize it are specified.
- A complete set of functions avoids pre-selected solutions.
- Product integration is improved.

Functional Analysis is an iterative process that works with and depends on the Requirements Development process, as shown in Figure 16. Functional Analysis begins with a high-level need and repeats through successively more detailed layers of decomposition until there is enough insight into the system's desired behavior to completely and correctly define the functional requirements. The highest-level needs are described in NAS-level ConOps (e.g., NextGen ConOps). High-level functions for the NAS ConOps are identified and decomposed to the lowest level. The functional requirements associated with these functions or their derivatives will be allocated to the system and become part of the Solution ConOps from which lower-level system functions will be identified and decomposed. The system functions are sent to the Requirements Management process, where the system functional and performance requirements are developed and documented in the preliminary Program Requirements Document (pPRD).

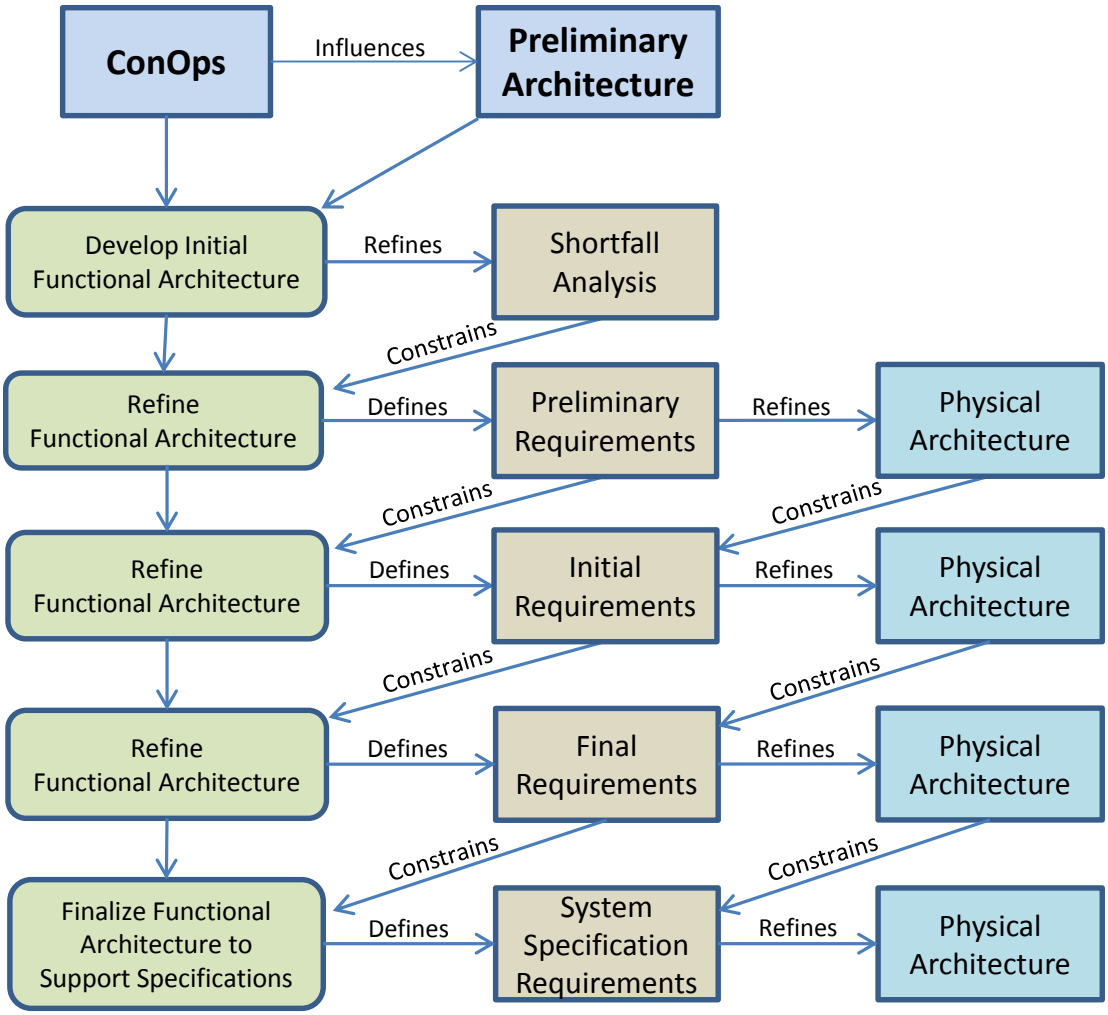


Figure 16: Functional Analysis, Requirements Management, and Design Solution Processes

Figure 17 provides a high-level summary of the functional analysis process.

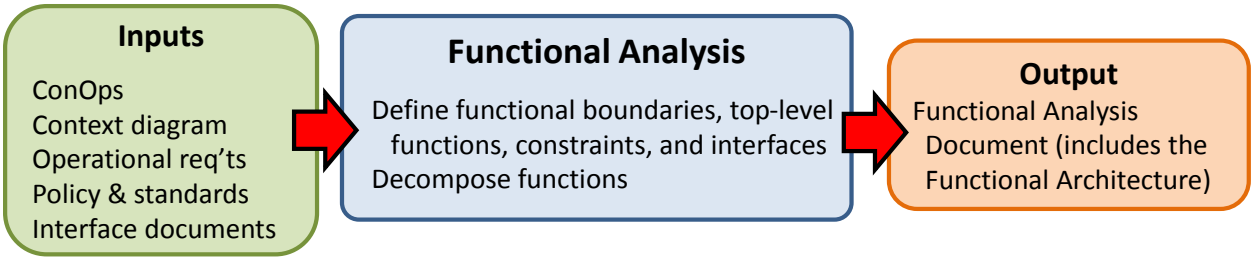


Figure 17: Functional Analysis Inputs, Activities, and Output

3.2.1 Inputs

The inputs, as shown in Figure 17, required for the Functional Analysis will vary, depending on the scope of a given effort and the iteration of the process. Based on the Operational Concept process output, the primary inputs (at the highest level) are the following:

- Concept of Operations (ConOps) document
- Operational Context Diagram (typically found in the ConOps)
- NAS-level operational requirements
- Policy and standards
- Interface control documents
- Legacy system documentation (if applicable)

Concept of Operations (ConOps)

The ConOps document encompasses the results of the Operational Concept Development activity and is intended to describe a new solution's operational characteristics from the user's point of view (i.e., stakeholder expectations). The ConOps document defines the way the solution will be used and involves input from a broad range of stakeholders, such as operations, maintenance, and management personnel. The document also indicates any critical, top-level performance requirements or objectives and solution rationale. The term ConOps is used for all levels of concepts from the enterprise- or NAS-level to the solution level. The solution level is frequently also referred to as the "system-level", although the developed solution is not always a system.

Operational Context Diagram

To define the problem from a functional standpoint, one must first review all existing inputs and required outputs to obtain a complete understanding of the mission and the top-level functions, environments, requirements, imposed constraints, and boundaries. A starting point for functional analysis is the operational context diagram which is usually contained in the ConOps document. The operational context diagram shows the expected solution boundaries, external entities that interact with the anticipated solution, and the relevant information flows between these external entities and the proposed solution. Understanding the potential inputs and outputs ensures consideration of the solution's relationship to its environment and to external solutions during development of the primary functions.

Operational Requirements

Operational Requirements are high-level requirement statements that identify the critical capabilities needed in a system to fulfill a specific mission for a stakeholder. Operational requirements derived from a higher-level ConOps or enterprise-level Operational Requirements Document (ORD) are allocated to the solution(s) and included in solution-level ConOps.

Policy and Standards

All relevant laws; agency policy, standards, and orders; as well as any applicable industry standards are constraints to the functional analysis and eventual solution-level requirements.

Interface Documents

The proposed solution will need to interface with existing systems in order to function. These interfaces are constraints to the functional analysis and eventual solution-level requirements.

3.2.2 Process Components

The following sub-sections describe, at a relatively high level, how to perform functional analysis and the various techniques for diagramming functional behavior of a solution. For more detail, refer to the *Functional Analysis Handbook*.

3.2.2.1 Perform Functional Analysis

The Perform Functional Analysis process establishes and documents a definition of required functionality. Functional analysis must be performed without consideration for a design solution or as it is more often known, "implementation-free." There are three primary reasons for conducting a functional analysis. First, it decomposes the functions to lower-level functions that will be satisfied by elements of the system design (e.g., subsystems, components, or parts); second, it identifies relationships between multiple system functions and between system functions and external users; and third, it leads to a complete set of functional requirements.

In the Functional Analysis process, the highest-level functions are identified from the ConOps, and then are further refined through functional decomposition to the lowest level to provide a basis for identifying and assessing design alternatives. The decompositions result in a set of basic sub-functions, and each sub-function at the lowest level can be instantiated into a valid set of functional requirements via the Requirements Development process. The FAA Functional Analysis process incorporates high-level activities and additional lower-level activities as below.

1. Define the functional boundary of the system in terms of the behavior and properties to be provided. The scope of this sub-process includes the system's stimuli and its responses to user and environment behavior. The result establishes the expected system behavior, expressed in quantitative terms, at its boundary.
    - Review all existing inputs to obtain a complete understanding of the top-level missions/functions, environments, requirements and imposed constraints.
    - Identify stakeholders to include the system engineer(s) responsible for the service or system, the system engineer(s) responsible for related cross-cutting disciplines, and the lead for any higher-level Functional Analysis effort.
    - Document assumptions to validate with stakeholders.
2. Identify and document each top-level function that the system is required to perform. These functions are what the proposed system must do to accomplish its operational mission and stakeholder expectations and not how it will accomplish them. The best way to identify these functions is to analyze the systems inputs and outputs captured in the context diagrams.
    - Organize top-level functions into logical relationships by creating a functional hierarchy (see Figure 18) and using Functional Flow Block Diagrams and N^2 diagrams.
    - Decompose top-level functions to the lowest level possible with available information.
    - Evaluate alternative decompositions.
    - Develop lexicon that defines the functions and data elements identified as providing required system capability.
    - Develop a Functional Flow Block Diagram and N^2 diagram for each level of the hierarchy.
3. Define necessary implementation constraints that are introduced by stakeholder expectations or that are unavoidable solution limitations (e.g., FAA standards).
4. Define the external interfaces and all functional interfaces. The interfaces are identified and their functional interactions are defined, such as start and end states or inputs and outputs.
5. Verify the results of functional analysis against the Concept of Operations. Some derived functions will be at a lower level than the ConOps, so they can only be validated by the stakeholders.
6. Validate the results of the functional analysis against the Stakeholder Expectations.
7. Document the Functional Analysis in a Functional Architecture Document, as described in the Outputs sub-section.

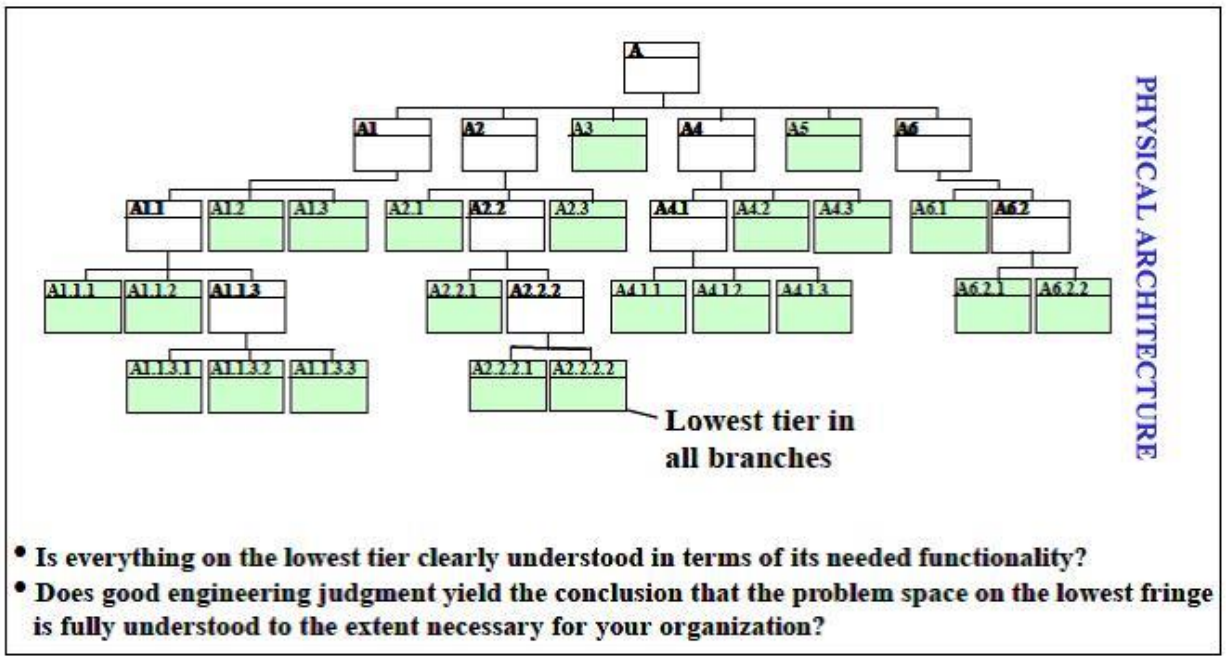


Figure 18: Functional Hierarchy

3.2.2.2 FAA-Preferred Diagramming Techniques

The FAA prefers using the complementary Functional Flow Block Diagram (FFBD) and N-squared ($N^{2)}$ diagramming techniques for documenting the functional behavior of a system. A complete functional model must depict both the "control" and "data" aspects of the system, represented by the FFBD and N^2 diagrams, respectively. Note that FFBD is preferred for systems engineering, whereas the SV-4 diagram represents similar information and is part of the enterprise architecture package.

Functional Flow Block Diagrams

The FFBD is a multi-tier, time-sequenced, step-by-step diagram of the system's functional flow. An FFBD usually defines the detailed, step-by-step operational and support sequences for systems, but one may also be used effectively to define processes when developing and producing systems. The software development processes can also use FFBDs extensively. In the system context, the functional flow steps may include combinations of hardware, software, personnel, facilities, and/or procedures. In the FFBD method, the functions are organized and depicted by their logical order of execution. Each function is defined as a verb-noun pair and is shown with respect to its logical relationship to the execution and completion of other functions. A node labeled with the function name depicts each function. Arrows indicate the order of execution of the functions. Logic symbols represent sequential or parallel execution of functions

A key concept in modeling functional flow is that for a function to begin, the preceding function or functions within the "control" flow must have finished. For example, a "display targets" function logically would not begin until a "detect targets" function was completed. The logical sequence of functions (i.e., the functional flow) describes the "control" environment of the functional model. In addition to a function being enabled, it may also need to be triggered with an input. So, in the example, the "display targets" function is enabled once the "detect targets" function is completed, and once it receives the "transmit radar signal" as input. This second aspect—triggering a function—speaks to the "data" environment, which the N^2 diagram captures.

Most system functionality can be modeled using the standard symbols discussed below. If an extended set of symbols is required, then it should be defined in the resulting Functional Analysis Document (FAD) to ensure that all stakeholders are able to accurately interpret the diagrams.

Function Symbology

A function shall be represented by a rectangle containing the title of the function (an action verb followed by a noun phrase) and its unique decimal delimited number. A horizontal line shall separate this number and the title, as shown in see Figure 19. The figure also depicts how to represent a reference function, which provides context within a specific FFBD.

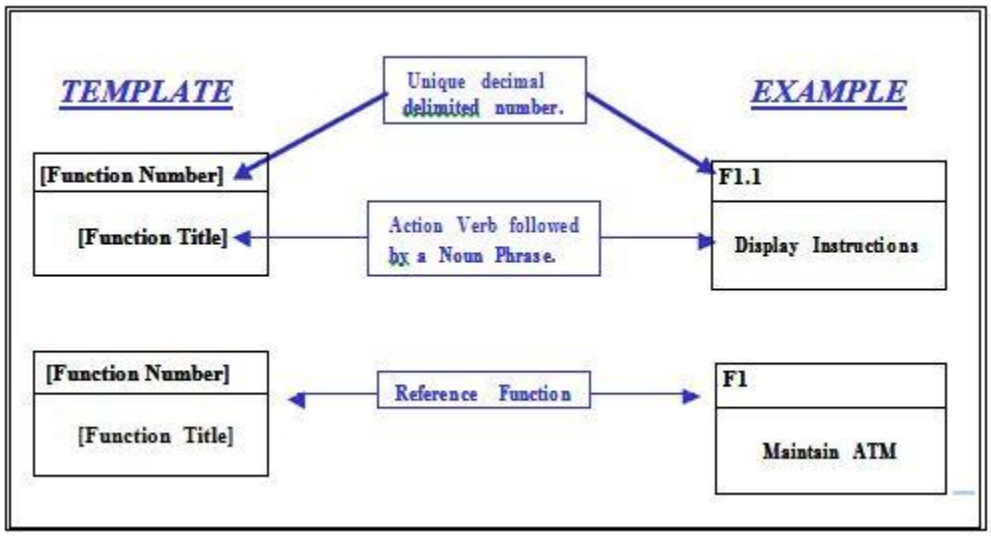


Figure 19: Function Symbol

Directed Lines

A line with a single arrowhead shall depict functional flow from left to right, as shown in Figure 20.

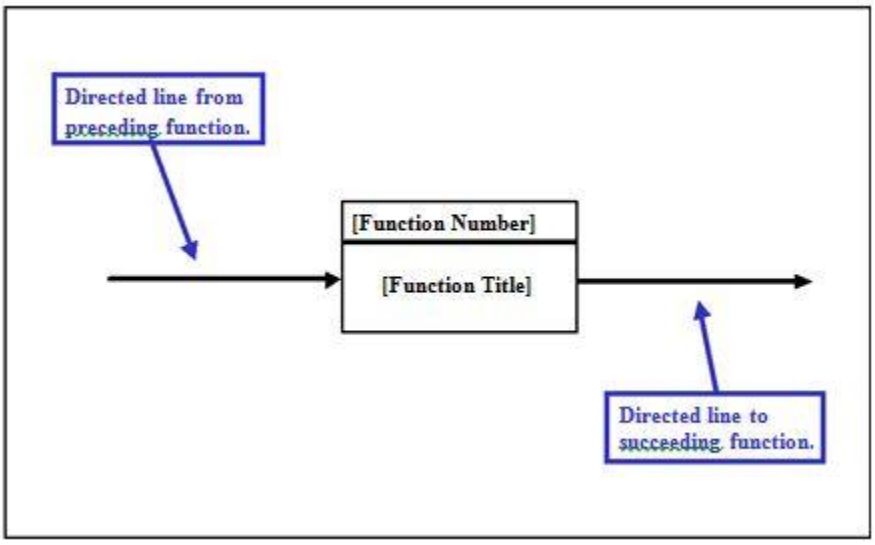


Figure 20: Directed Lines

Logic Symbols

The following basic logic symbols shall be used:

- **AND**: A condition in which all preceding or succeeding paths are required. The symbol may contain a single input with multiple outputs or multiple inputs with a single output, but not multiple inputs and outputs combined (Figure 21). Read the figure as follows: F2 **AND** F3 may begin in parallel after completion of F1. Likewise, F4 may begin after completion of F2 **AND** F3.

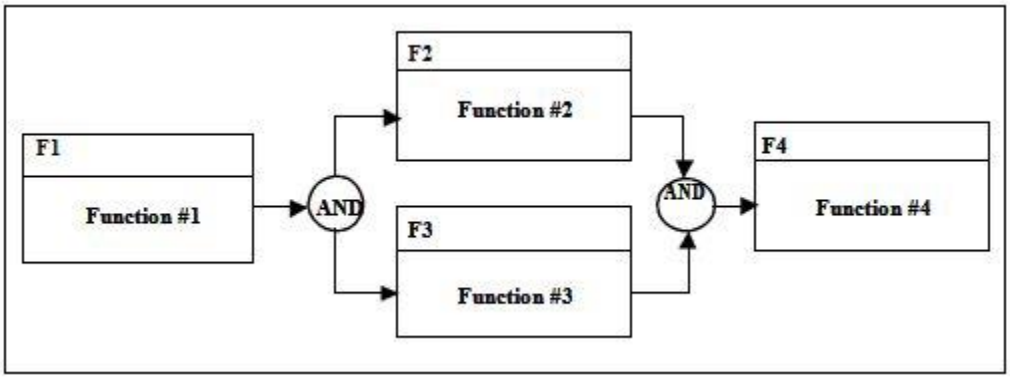


Figure 21: "AND" Symbol

- **Exclusive OR:** A condition in which one of multiple preceding or succeeding paths is required, but not all. The symbol may contain a single input with multiple outputs or multiple inputs with single output, but not multiple inputs and outputs combined (Figure 22). Read the figure as follows: F2 **OR** F3 may begin after completion of F1. Likewise, F4 may begin after completion of either F2 **OR** F3.

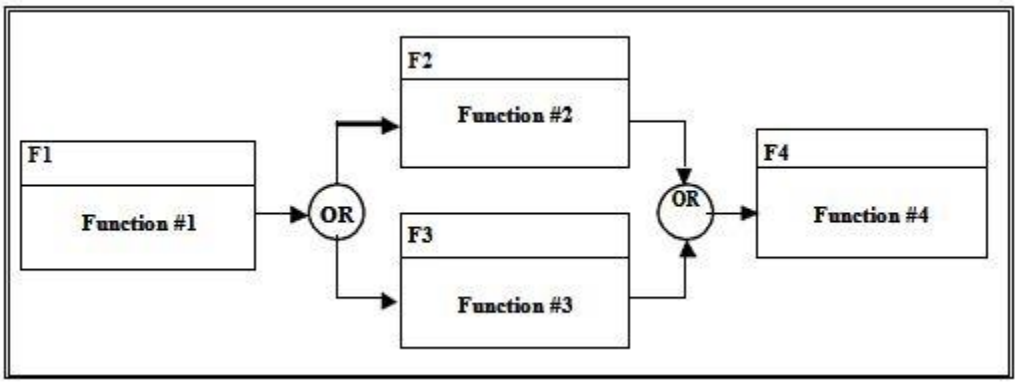


Figure 22: "Exclusive OR" Symbol

- **Inclusive OR:** A condition in which one, some, or all of the multiple preceding or succeeding paths are required. Figure 23 depicts **Inclusive OR** logic using a combination of the previously described **AND** and **Exclusive OR** symbols. Read Figure 23 as follows: F2 **OR** F3 (exclusively) may begin after completion of F1, **OR** (again exclusive) F2 **AND** F3 may begin after completion of F1. Likewise, F4 may begin after completion of either F2 **OR** F3 (exclusively), **OR** (again exclusive) F4 may begin after completion of both F2 **AND** F3.

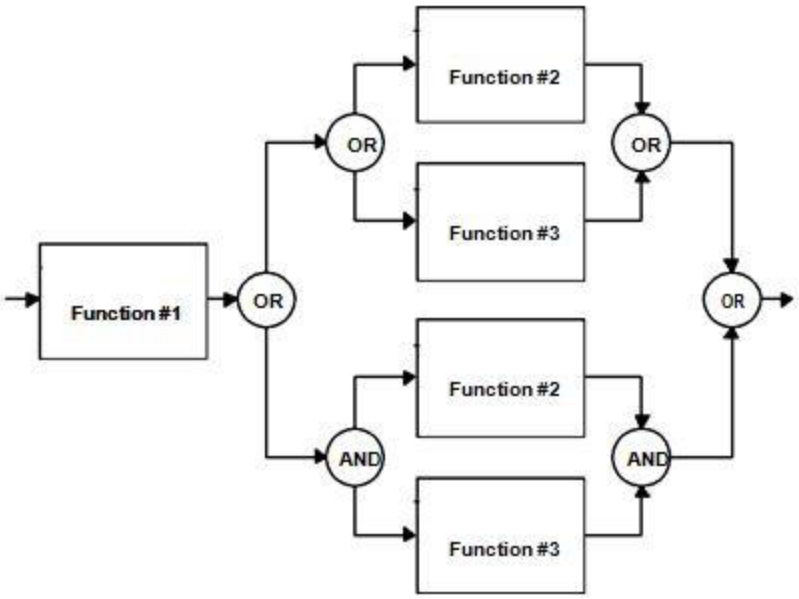


Figure 23: "Inclusive OR" Logic

Contextual and Administrative Data

Each FFBD shall contain the following contextual and administrative data:

- Date the diagram was created
- Name of the engineer, organization, or working group that created the diagram
- Unique decimal delimited number of the function being diagrammed
- Unique function name of the function being diagrammed

Figure 24 and Figure 25 present the data in an FFBD. Figure 25 is a decomposition of the function F2 contained in Figure 24 and illustrates the context between functions at different levels of the model.

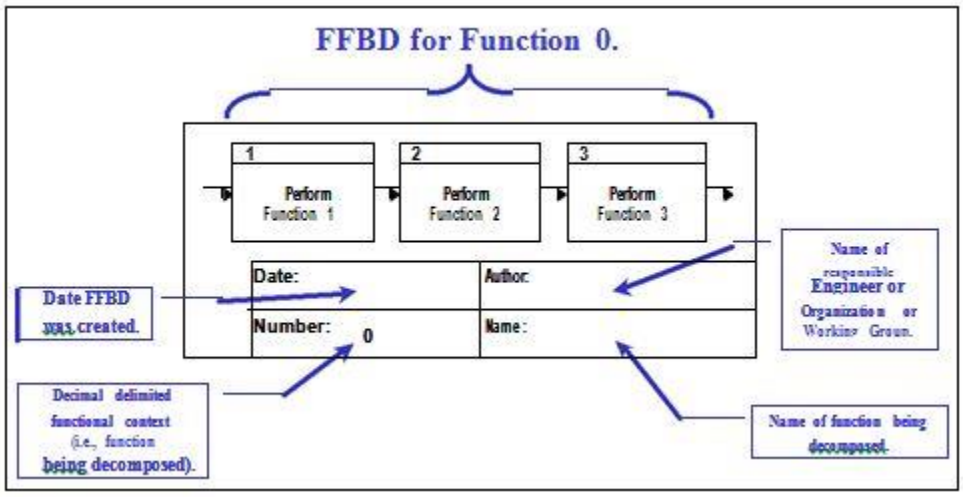


Figure 24: FFBD Function 0 Illustration

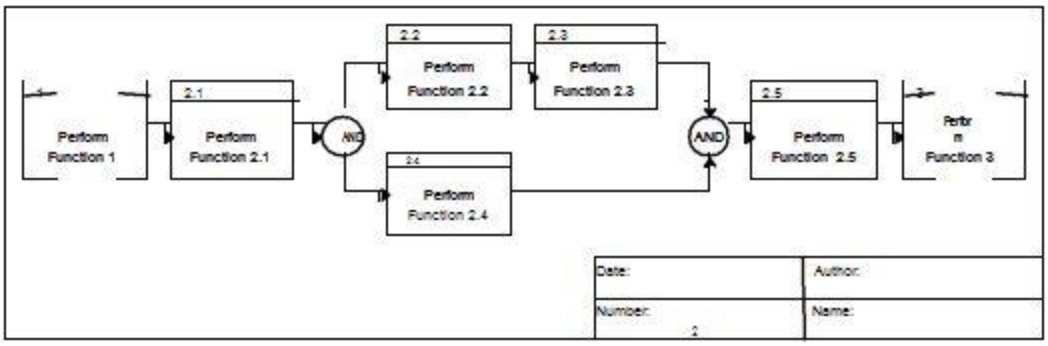


Figure 25: FFBD Function 2 Illustration

N-Squared (N^2) Diagramming

The N^2 diagram is a visual matrix representing functional or physical interfaces between system elements. It is used to systematically identify, define, tabulate, design, and analyze functional and physical interfaces. It applies to system interfaces and hardware and/or software interfaces. The "N" in an N^2 diagram is the number of entities for which relationships are shown. This NxN matrix requires the user to generate complete definitions of all interfaces in a rigid bidirectional, fixed framework. The user places the functional or physical entities on the diagonal axis and the interface inputs and outputs in the remainder of the diagram squares. A blank square indicates that there is no interface between the respective entities.

Data flows clockwise between entities (i.e., the symbol F1 (arrow) F2 in Figure 26 indicates data flowing from function F1 to function F2; the symbol F2 (arrow) F1 indicates the feedback). That which passes across the interface is defined in the appropriate squares. The diagram is complete when the user has compared each entity to all other entities. The N^2 diagram should be used in each successively lower level of entity decomposition. Figure 26 illustrates directional flow of interfaces between entities within an N^2 diagram. (In this case, the entities are functions.)

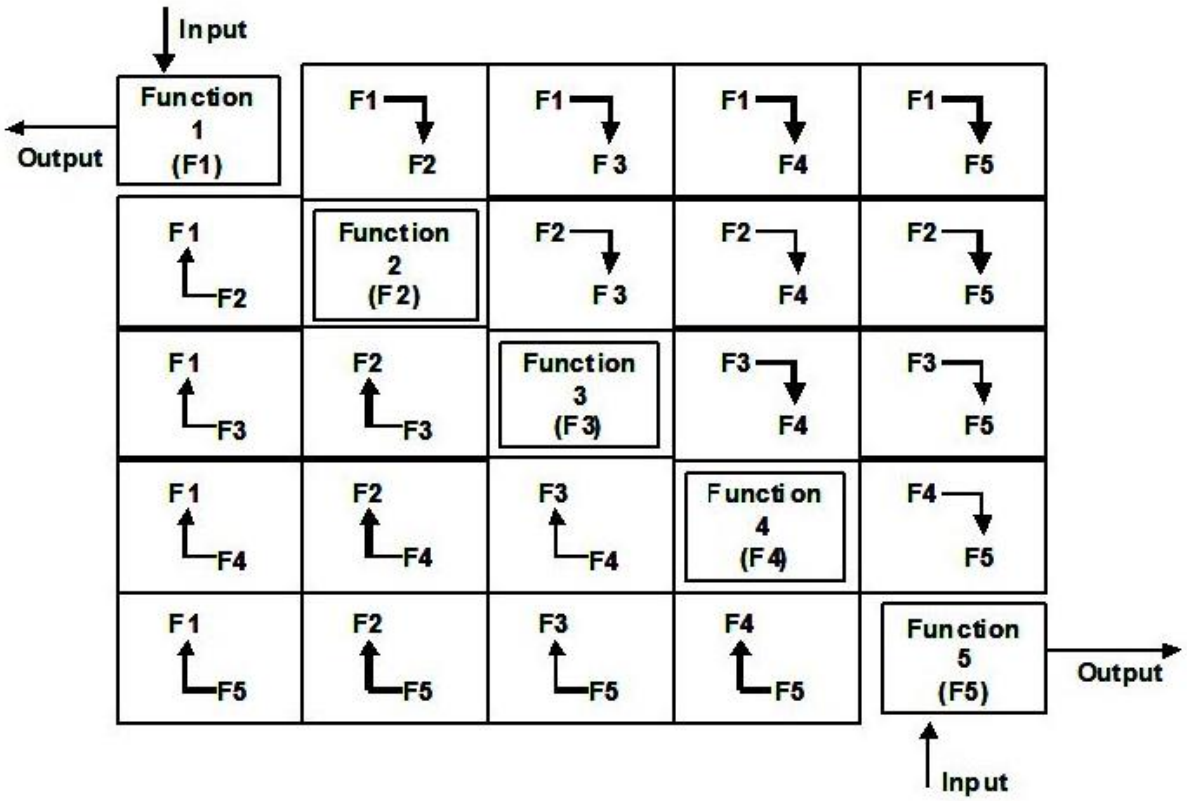


Figure 26: N^2 Diagram Flow

In the above example, N equals 5. The five functions are on the diagonal. The arrows show the flow of data between functions. So if Function 1 sends data to Function 2, the data elements would be placed in the box to the right of Function 1. If Function 1 does not send data to any of the other functions, the rest of the boxes to right of Function 1 would be empty. If Function 2 sends data to Function 3 and Function 5, then the data elements would be placed in the first and third boxes to the right of Function 2. If any function sends data back to a previous function, then the associated box to the left of the function would have the data elements placed in it. The squares on either side of the diagonal (not just adjacent squares) are filled in with appropriate data to depict the flow between the functions. If there is no interface between two functions, the square that represents the interface between the two functions is left blank. Physical interfaces would be handled in the same manner, with the physical entities on the diagonal rather than the functional entities.

N^2 diagrams are a valuable tool for not only identifying functional or physical interfaces, but also for pinpointing areas in which conflicts may arise with interfaces so that system integration proceeds smoothly and efficiently.

Each N^2 diagram shall contain at a minimum the following contextual and administrative data:

- Date the diagram was created
- Name of the engineer, organization, or working group that created the diagram
- Unique decimal delimited number of the functional or physical entity being diagrammed
- Unique name for the functional or physical entity being diagrammed

Figure 27 presents the information in an N^2 diagram, which complements the FFBD (Figure 24 above).

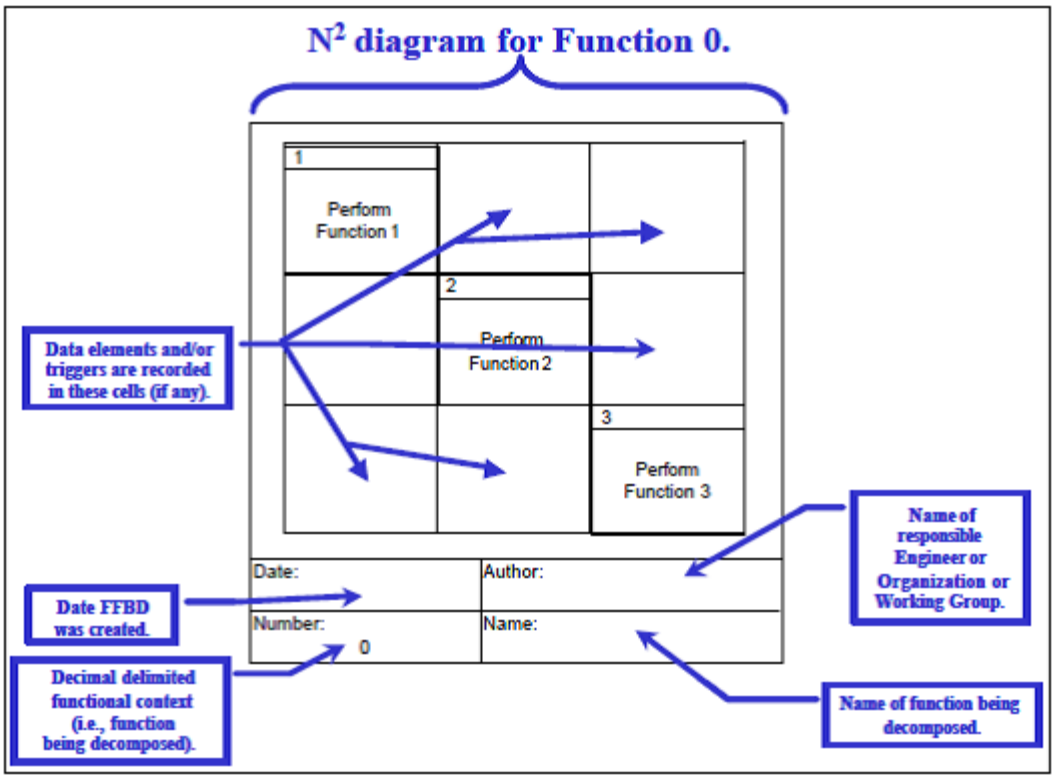


Figure 27: N^2 Diagram example

Figure 28 complements the FFBD illustrated in Figure 25 above, and is an example of the diagram's appearance when cells are populated with data.

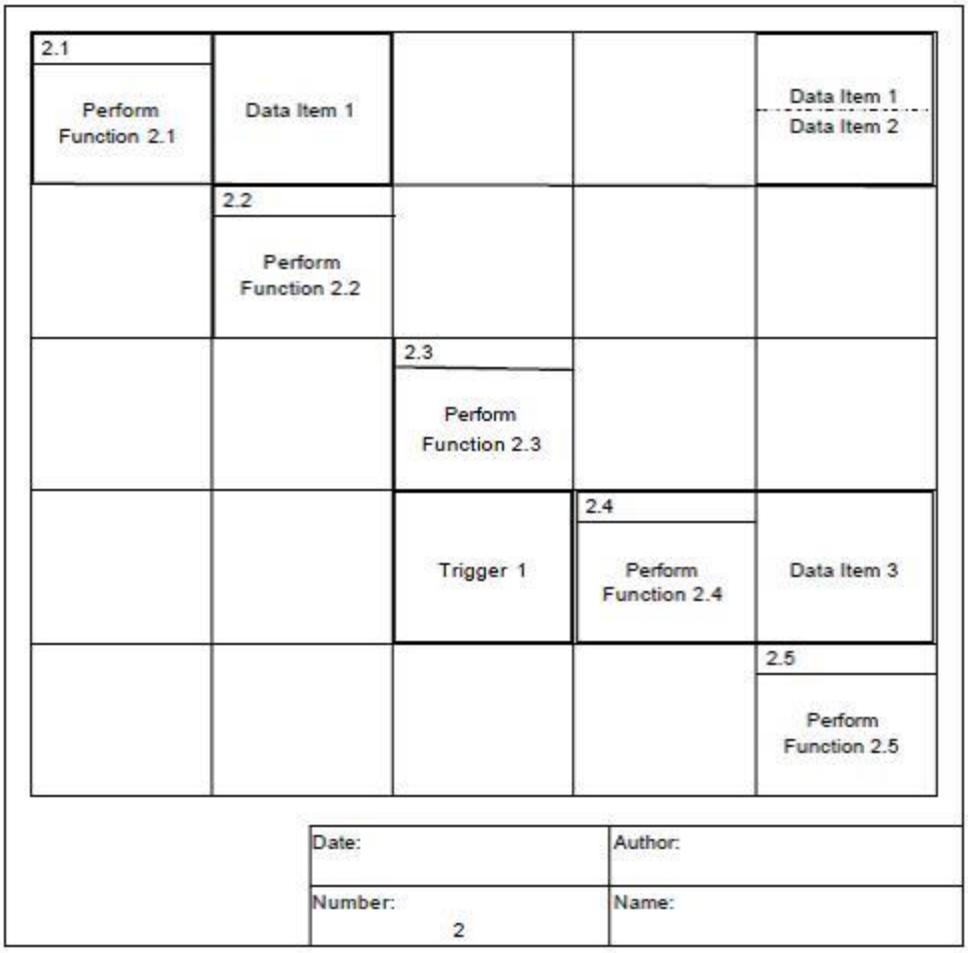


Figure 28: N^2 Diagram Illustration No. 2

3.2.3 Outputs

Functional Architecture

The Functional Analysis process produces a Functional Architecture Document, which consists of seven parts:

1. **Context Diagrams**: shows the low-level functional system boundaries, external entities that interact with the anticipated system, and the relevant information flows between these external entities and the proposed system. The major distinction between this context diagram and the operational context diagram is the increased level of functional detail.
2. **Functional Hierarchy**: a hierarchical arrangement of functions that represents the complete system. The process moves to a greater level of detail as the identified functions are further decomposed into sub-functions. Functional decomposition reduces complexity by allocating functionality and interfaces to more readily understood and managed sub-level functions. This process is repeated until the system is completely decomposed into basic sub-functions, and each sub-function at the lowest level is instantiated into a valid set of requirements.
3. **Functional Flow**: a multi-tier, time-sequenced, step-by-step diagram of the system's functional flow that defines the detailed, step-by-step operational and support sequences for the system under consideration. The preferred engineering documentation method is Functional Flow Block

Diagrams. However, documentation can also be achieved by IDEF0 diagrams or SV-4 diagrams, an enterprise architecture product.

4. **N^2 Diagrams**: a visual matrix representing functional or physical interfaces between system elements and associated data flows.
5. **List of Functional Interfaces**: shows the relationship between multiple functions which were derived from the functional hierarchy. The interfaces between each of the functions and sub-functions are fully defined, as are the interfaces to the environment and external systems. The resulting functional architecture may be represented as an N^2 diagram.
6. **Lexicon**: identifies all nouns and verb phrases used to specify functions.
7. **Acronyms and Abbreviations** used in the Functional Analysis Document.

The recommended outline for the Functional Analysis Document (FAD) is shown below

1.0: Introduction

1.1: Summary of the Concept of Operations

1.2: Operational Concept

1.3: System Bounds

1.4: Time Frame

2.0: Operational Context

2.1: High Level Context Diagram

2.2: High Level Context Functions

2.3: Boundary Systems

2.4: Boundary Users

2.5: Operational Environment

3.0: Functional Architecture

3.1: Functional Hierarchy

3.2: Functional Interfaces Description

3.3: Functional Flow Diagrams

3.4: N^2 diagrams

4.0: References

5.0: Definitions

6.0: Acronyms

Description of Diagrams

- **N^2 Diagram** – An N^2 diagram or N^2 chart is a matrix structure that depicts the inputs, outputs, and functions of a system. This system engineering tool is used for tabulating, defining, analyzing, and describing functional interfaces and interactions among system components. The elements of the diagram are at the same level of hierarchical decomposition. The diagram is constructed so functions are represented in boxes down the diagonal and illustrate the inputs and outputs between each function.
- **Functional Flow Block Diagram** – Functional Flow Block Diagrams illustrate the control structure that dictates the order in which the functions can be executed at each level of decomposition.

- **IDEF0 Diagram** – The Integrated Definition for Function Modeling (IDEF0) is a process for modeling how inputs are transformed into outputs via some function. The resulting artifacts are called IDEF0 diagrams. An IDEF0 diagram can represent any level of system abstraction, and at least two diagrams are needed per system. The first IDEF0 diagram, known as page A-0, depicts the context diagram with the inputs, controls, outputs, and mechanisms for the top-level function of the system. This diagram establishes the scope and boundaries of the system and indicates interacting external systems. The remaining IDEF0 diagrams represent a decomposition of a function from a higher level of abstraction, starting with the function identified in A-0. The operational activity model (OV-5) that can be used to help determine system functions is an IDEF0 diagram.
- **SV-4** – The SV-4 is an enterprise architecture artifact that illustrates functions performed by systems and the system data flows among system functions. The results of the functional analysis directly contribute to the development of the SV-4 artifact.

3.2.4 Functional Analysis through the Life Cycle

In the FAA, functional analysis is largely accomplished during the Service Analysis & Strategic Planning and CRD phases. The main outcome of functional analysis is the Functional Architecture which is then used to develop system-level requirements as well as the solution architecture. Therefore, requirements documents and architecture products need to be in alignment with the Functional Architecture. Since programs may need to change or add functionalities or requirements which may not have been documented in the FAD, the functional analysis documented in the FAD should be updated during the Investment Analysis, Solution Implementation and In-Service Management phases.

Service Analysis and Strategic Planning

Preliminary work on the Functional Analysis can begin during the Service Analysis phase, where the Recommended Changes to Enterprise Architecture and Preliminary Shortfall Analysis are two major products. Functional Analysis process can support these two products by:

- Defining the preliminary functional boundary of the system in terms of the functions that need to be provided.
- Identifying a preliminary set of top level functions that are needed to support the Shortfall Analysis
- Identifying if the required top level functions are represented in the current Enterprise Architecture views, primarily the SV-4. If not, determine if the SV-4 views need to be amended.

Concept and Requirements Definition

The bulk of the Functional Analysis is done during the Concepts and Requirements Definition phase. During this phase the final FAD is produced and gets reviewed by the JRC. The approved FAD forms the starting basis for aligning the preliminary requirements and the SV-4 architecture view. Steps in the Functional Analysis process during this phase include:

1. Refine the functional boundary of the system in terms of the behavior and properties to be provided, including the system's stimuli and its responses to users and environmental behavior.
2. Refine the top level functions into set of lower level functions that fully describe what the system will achieve in fulfilling a particular operational mission while being solution agnostic. This step will include creating a detailed hierarchy, FFBD and N^2 diagrams as well as a detailed Lexicon. Also included in this step is the development of alternative functional decompositions to support the evaluation of a range of architectures. These will be documented in the FAD as a formal deliverable.
3. Identify the constraints imposed upon the Functional Architecture including standards, regulations, environmental conditions and stakeholder requirements.
4. Identify all external and functional interfaces.

5. Verify the Functional Analysis against the ConOps.
6. Validate the Functional Analysis with the customer.

Investment Analysis

Once the FAD is approved by the JRC during IARD, it should not be left in isolation while requirements and the architecture are evolved. As new requirements are identified and updated in the iPR during IIA and in the fPR during FIA, the FAD also needs to be evaluated for updates. Similarly as new functionalities or interfaces are identified in the architecture views, the FAD needs to be evaluated for updates. The main goal of this process is to ensure that the Functional Analysis as documented in the FAD is in alignment with the requirement documents and architecture views which eventually are submitted for contract solicitations. The following Functional Analysis steps need to be done during this phase:

1. Update the Context Diagram in the FAD with any newly identified external boundaries to the system.
2. Update the functional hierarchies and the FFBDs in the FAD with any updates to the functions identified during the requirements and architecture development process which may trace up to the higher level functions.
3. Update the FAD with newly identified constraints imposed upon the Functional Architecture.
4. Update the N^2 diagrams in the FAD with any newly identified external and functional interfaces.
5. Verify the updates to the FAD against the ConOps.
6. Validate the updates to the FAD with the customer.

Solution Implementation

During the Solution Implementation phase, programs may make changes to requirements and specifications that affect the functions described in the Functional Analysis. Programs should update the Functional Analysis Document to reflect the changes. Contractors are likely to play a significant role in functional analysis at this point in the lifecycle.

In-Service Management

In the FAA, Tech Refresh and System Life Extension Programs (SLEP) are commonly used to extend the capabilities of an existing system due to new stakeholder needs, changing boundary conditions or new constraints. If during the In-Service Management phase, a program makes changes to a system, its interfaces, or boundaries, an assessment should be made as to whether or not these changes trace up to a high enough level where it can impact the Functional Analysis. If they do, the FAD should be updated with the new information.

Additional Information

For sources of information used to generate content throughout this section, see References.

To learn more about the topics in this section, see Additional Tools and Reading Recommendations.

3.3 Requirements Analysis

Requirements Analysis is performed throughout a system's life cycle to elicit, identify, develop, and manage requirements. A **requirement** is an essential characteristic, condition, or capability that is to be met or exceeded by a system or component to satisfy standards, a contract, specification, or other formally imposed document. A **requirements set** is an aggregate set of requirements that is developed, documented, and baselined for the identified system.

Requirements Analysis is an iterative process that defines the essential system characteristics for all system components required for the product's successful development, production, deployment, operation, and disposal. Requirements Analysis works in conjunction with Functional Analysis and Architectural Design Synthesis to generate requirements for a program or project throughout its life cycle. Requirements Analysis is comprised of two distinct activities:

- Requirements Development
- Requirements Management

Requirements Development develops functional requirements from the functions developed through the Functional Analysis Process. It also elicits and identifies system-specific characteristics based on analyses of stakeholder needs, objectives, missions, constraints, and measures of effectiveness. These characteristics are used to develop consistent, traceable, and verifiable performance requirements and associated documentation. Requirements Development works with Architectural Design Synthesis to allocate requirements to the appropriate component within the system hierarchy and/or the appropriate organizational entities (e.g., to develop procedures).

Requirements Management manages and controls requirements and associated documentation throughout the project lifecycle. It ensures solution compliance with stakeholder needs and expectations.

Requirements Analysis is applicable at both the NAS and system level. It is important to note that a set of program requirements should be stable prior to committing to a full investment. If many requirements are still under development and the requirements set is in flux, then the program is not ready to proceed into system design.

3.3.1 Requirements Development

Requirements Development is the determination of system-specific characteristics based on analyses of stakeholder needs, objectives, missions, constraints, and measures of effectiveness. Figure 29 describes the inputs, processes, and outputs of Requirements Development.

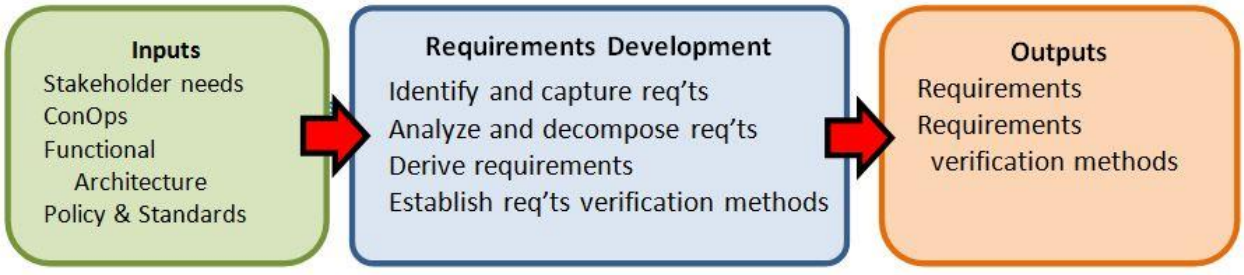


Figure 29: Requirements Development Inputs, Processes, and Outputs

3.3.1.1 Inputs

The primary inputs to the Requirements Development process are as follows:

- Stakeholder needs
- ConOps document
- Functional Architecture
- Policy and standards

Stakeholder Needs

Systems engineering commences when a mission goal or need is identified in the form of a new or improved capability, or identified shortfall. Needs are identified during gap analysis and may result from executive directives, new laws, ordinances or legislative directives. Studies resulting from operational issues may also identify needed capabilities or operational improvements. Impacted stakeholders provide subject matter expertise in order to clearly identify and document all stakeholder needs. Stakeholder needs help to define operational requirements and top-level performance metrics. They are also used in the verification of requirements.

ConOps

A Concept of Operations (ConOps) is a description of what is expected from the system. The ConOps document defines the way the system will be used and involves input from a broad range of stakeholders, such as operations, maintenance, and management personnel. The ConOps describes the existing system, current environment, users, interactions between users and the system, and organizational impacts. The functions described in the ConOps are the first input to the "capture requirements" step of Requirements Development. As Requirements Management iterates, the ConOps is further decomposed using functional analysis to refine requirements.

Functional Architecture

The functional architecture is a hierarchical arrangement of functions and interfaces that represents the complete system, as described in Section 3.2: Functional Analysis. Every function required to satisfy a system's operational needs is identified and defined. Once defined, the functions are used to define system requirements. Requirements Development uses the functional architecture to develop requirements for internal and external interfaces.

Policy and Standards

Relevant agency policies as well as applicable industry standards are input as constraints or passive requirements for the system. A standard is a document that establishes engineering and technical requirements for processes, procedures, practices, and methods that have been adopted as standard. Standards may also establish requirements for selection, application, and design criteria. Sources include government regulations and statutes, international policy, and FAA policy. Examples of policy include government statutes impacting the system, including requirements incorporated into Executive Orders and legislation, or ICAO Standards and Recommended Practices (SARP). FAA policy may include technical, operational, acquisition, financial, and other requirements.

3.3.1.2 Process Components

There are four main sub-processes needed to accomplish the Requirements Development process:

1. Identify and capture requirements
2. Analyze and decompose requirements
3. Derive requirements
4. Establish requirements verification methods

The four sub-processes are iterative and may occur in parallel. They are detailed below.

1. Identify and Capture Requirements

Requirements are an integral part of any project. Utilizing the criteria established in the Requirements Management Plan – described in Integrated Technical Planning – this sub-process identifies, prioritizes, and extracts all stakeholder needs. This process is performed on the entire system, including any known operational performance needs and constraints. The following steps support the identification and capture of requirements:

a) Define Stakeholder Needs. Stakeholder needs in the FAA come from the operational stakeholder in the form of a ConOps or shortfall and opportunity analysis. They are transformed into baseline requirements sets at a successively lower level through iteration of the Requirement Development process. It is recommended that the definition of stakeholder needs be balanced with an analysis of their effects on the overall system design and performance. Stakeholder needs include:

- What the system is to accomplish (functional requirements)
- How well each function is to be performed (performance requirements)
- The operational and ambient environment in which the system is to be operated
- Constraints under which the system is to be developed or operated (e.g., policy, procedures, funding, schedule, technological maturity.)

b) Define Constraints. The Systems Engineer must identify and define constraints that impact design solutions. The NAS Enterprise Architecture may also impose long-range planning constraints through the approved capabilities and operational improvements. Some examples of constraints include:

- Interfacing systems
- Existing approved specifications and baselines
- Environmental constraints
- Availability of automated tools
- Required Metrics for measuring technical progress
- Constraints derived from other SE processes, including cost, schedule, programmatic, technology, and design constraints, and Earned Value Management variances
- FAA-wide general specifications, standards, handbooks, and guidelines
- FAA policy directives
- US Government and international laws and regulations
- Industry, international, and other general specifications, standards, and guidelines
- ICAO Standards and Recommended Practices (SARPs)
- Human-related specifications, standards, and guidelines
- Safety constraints

c) Define Operational Scenarios. Systems Engineers must identify and define scenarios that capture the range of the anticipated system uses. For each operational scenario, expected interactions with the environment and other systems, human tasks and task sequences, and physical interconnections with interfacing systems and platforms are defined. The ConOps and the NAS EA provide information for the scenarios.

d) Define Measures of Effectiveness. Measures of Effectiveness (MOE) are metrics used to measure results achieved in the overall mission of an investment. They identify the most critical performance requirements to meet system-level mission objectives and will reflect key operational needs. Data for this step comes from the ConOps, pPRs and fPRs, the NAS

Enterprise Architecture, the NAS-level requirements, and operational scenarios. Measures of Performance (MOP), which are expressed as distinctly quantifiable performance features that are related to the achievement of MOEs are also defined. MOEs measure the outcome, where MOPs measure the outputs.

e) Define Interfaces. Systems Engineers must identify the functional and physical interfaces for the system. Functional and physical interfaces may include mechanical, electrical, thermal, data, communication, procedural, and human-machine interactions. These interfaces are either internal or external to the system. Internal interfaces address elements inside the boundaries established for the system. External interfaces involve relationships to entities outside the established system boundaries. Functional interfaces are obtained from the Functional Analysis Process. Architecture Systems Interface Description (SV-1) and Interface Requirements Documents (IRDs) are used to identify physical interfaces.

f) Define Utilization Environment. All environmental factors – operational and ambient- that may impact system performance are identified and defined. Also identified are factors that ensure that the system minimizes the potential for human or machine errors or for failures that cause accidents or death.

g) Define Life Cycle Process Concepts. Based on the needs that are defined lifecycle process requirements needed to develop, produce, test, distribute, operate, support, train, and dispose of system products being procured are developed. These requirements include manpower, personnel, training, human engineering, and safety.

h) Define Modes of Operation. The system modes of operation (e.g., full system, emergency, training and maintenance) are defined for the system being procured. The conditions (e.g., environment, configuration and operation) that determine the modes of operation are defined.

i) Define Technical Performance Measures. Technical Performance Measures (TPM) are defined that describe the key indicators of system performance. *TPMs are derived directly from the MOPs and are selected because they are critical for controlling and periodically reviewing performance.* TPMs help assess design progress, assess compliance to requirements throughout the WBS, and assist in monitoring and tracking technical risk. They can identify the need for deficiency recovery and provide information to support cost-performance sensitivity assessments. Examples of TPMs include range, accuracy, weight, size, availability, power output, power required, process time, and other product characteristics that relate directly to the system operational requirements.

It is recommended that selection of TPMs be limited to critical measures of performance that, if not met, put the project at cost, schedule, or performance risk. Specific TPM activities are integrated into the System Engineering Master Schedule to periodically determine achievement to date and to measure progress against a planned value profile.

2. Analyze and Decompose Requirements

This process translates the functional architecture developed in Functional Analysis into Primitive Requirements Statements (PRS) that are translated into Mature Requirements Statements (MRS).

The Functional Architecture is the primary input to the Requirements Development process; it is a hierarchical arrangement of functions and interfaces that represents the complete system. A Functional Architecture consists of functional flow block diagrams (FFBD), timeline sequence diagrams, and functional N-squared (N^2) charts, as described in Section 3.2: Functional Analysis. It is recommended that requirements be developed for every level of the Functional Architecture, as shown in Table 9.

Table 9: Functional Architecture to Requirements Traceability

Functional Architecture	Derived Product
ConOps	Preliminary Architecture
Functional Analysis 1	Preliminary Program Requirements
Functional Analysis 2	Initial Program Requirements
Functional Analysis 3	Final Program Requirements
Functional Analysis 4	System-level Specification
Functional Analysis N	System Specification to Nth Level

Initially, the systems engineer captures a PRS from a source appropriate to the level of the requirements document. A PRS is a primitive form of a requirement that has no punctuation or formal sentence structure. Each PRS is numbered according to the format of Name + Relation + Value. Table 10 provides examples of these relationships.

Table 10: PRS Examples

Name	Relation	Value	Units
Weight	less than or equal to	5120	Kilograms
Reliability	greater than or equal to	.998	(none)
Power output	greater than or equal to	100	Megawatts
Memory margin	greater than or equal to	100	Percent
Maximum turn rate	equal to	90	Degrees/min
Item screen refresh rate	equal to	20	Frames/sec
Input power	in accordance with	FAA-G-2100h	(none)

The name describes the characteristic or attribute to control, the relation details the connection between the attribute and its control value, and the value sets a quantifiable number with units or defines a standard. Relations for numerical requirements are described in one of six ways: less than, greater than, equal to, less than or equal to, greater than or equal to, or between a range of values.

The attributes from the PRS can be put together into a requirements statement, and additional attributes are captured. Unique identifiers and a reference for future verification can be added, as shown in Table 11. Each requirement must have a unique identifier for Configuration Management and traceability purposes. There must also be reference documentation to the source of the requirement for verification.

Table 11: Primitive Requirement Statements List

PRS Number	Primitive Requirement Statement	Functional Reference
Assign a unique number to the PRS	*This is the derived PRS*	*Assign the PRS to a function in the functional architecture*
126	Transmitter mean time between failure (MTBF) greater than 5,000 operating hours	F.3.2.1.1

The functional architecture and each existing PRS is reviewed and assigned to a function in the functional architecture. The list of developed PRS is sorted or grouped so that requirements allocated to an individual function are together. If additional functional requirements are developed that are not sourced from the functional architecture, the systems engineer must append the functional architecture to include this.

Mature Requirements Statements

After a PRS is identified, it is synthesized into a Mature Requirements Statement (MRS). An MRS is a requirement expressed in a complete sentence, in familiar language, and using the context of a particular business sector. A well-defined set of MRS needs to exhibit certain individual and aggregate characteristics. A PRS is converted into an MRS in specification text by adding the following characteristics:

- Paragraph number – the type of requirement is identified and a paragraph number is assigned in accordance with the FAA Acquisition System Toolset (FAST) template, FAA-STD-005.
- Paragraph title
- Subject
- Directive verb
- Sentence ending – the requirement sentence ends with a commonly used word or phrase that provides a reference to a standard or specification.
- Explanatory information – information to explain, define, or clarify is added after the requirements sentence if necessary to ensure understanding and avoid ambiguity.

Standard Requirements Constructs

Standard constructs are used to develop requirements. All requirements have directive verbs, commonly used words and phrasings that denote action, as follows:

- Shall – denotes compulsory or mandatory requirement or action that the system being directed is obliged to take
- May – denotes permission or an option that is not obligatory.
- Will – denotes a declaration of purpose on the part of the government
- Should – not to be used in requirements documents.
- Unless otherwise specified – used to indicate an alternate course of action.
- And/or – shall not be used in requirements documents
- Less than/ Greater than or equal to– shall be used in place of vague wording such as minimum or maximum

3. Derive Requirements

This activity identifies and expresses requirements that result from considering functional analysis, higher level requirements, constraints or processes. Requirements should be derived to the lowest practical level before being allocated to the physical architecture or Work Breakdown Structure (WBS) elements.

This activity clarifies or amplifies higher level requirements. These derived requirements need to be stated in measurable parameters at increasingly lower levels within the product hierarchy. Derived requirements may result from, but are not limited to, the following:

- Regulatory policies, program policies, agency practices, and supplier capabilities
- Environmental and safety constraints; the process translates and traces safety-specific system requirements into the software and hardware requirements baseline. Safety program requirements are also reflected in organizational standards and procedures.
- Architecture choices for performing specific system functions
- Design decisions
- Hardware-software interfaces not already specified in the baseline interface documentation
- Establishment of detailed requirement values and tolerances (i.e., minimum, maximum, goal, threshold)
- Impacts of derived requirements need to be analyzed progressively in all directions (parent, child, and peer) until it is determined that no additional impact is propagated. During this process, the hardware and software architecture design is reviewed for flexibility to adapt to new system requirements.

Derived requirements are captured and treated in a manner consistent with other requirements applicable during the development stage. This activity, like overall SE, is an iterative operation, constantly refining and identifying new requirements as the product concept develops and additional details are defined. As part of the requirements derivation process, areas of the system with volatile requirements are monitored, and requirements specifications are reviewed for ambiguities with the potential of causing software sizing and timing instability and other program impacts.

Figure 30 illustrates the FAA Requirements Development process flow that starts with the ConOps and ends with the System Specification that will be used for system acquisition. At any time during the process, the functions and requirements at a higher level can be revisited and reworked as necessary. These changes will then propagate downward until the lower levels reflect the changes.

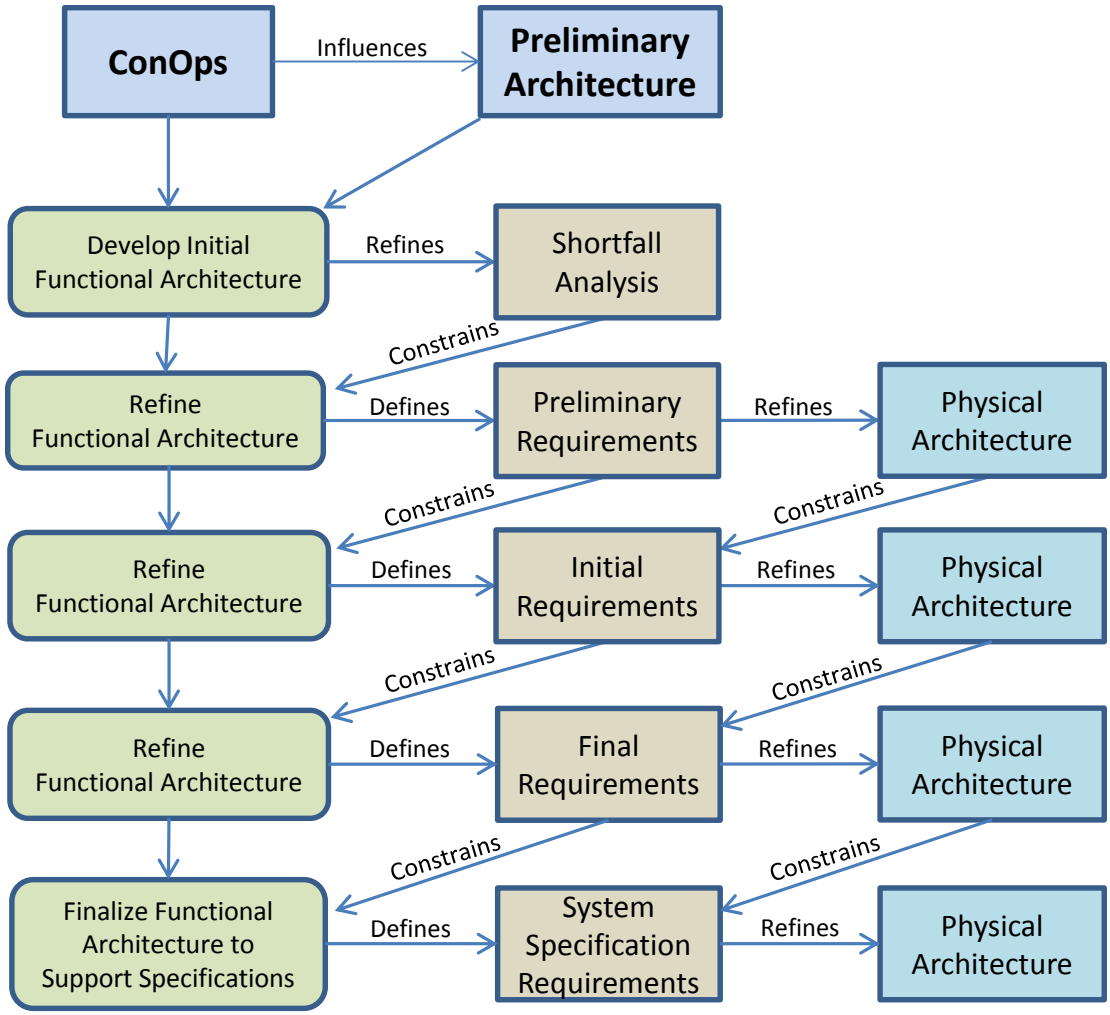


Figure 30: FAA Requirements Development Process Flow

Characteristics of Individual Requirements

Characteristics of individual requirements may be used for requirements development as well as in requirements reviews and audits for assessing the quality of requirements. Proper requirements exhibit the following characteristics:

- Necessary – the requirements is an essential capability, characteristic, or quality factor of the product or process. A good test of necessity is whether the requirement can be traced to higher level documentation; if there is no parent requirement, it may not be necessary.
- Concise / minimal / understandable – the statement includes only one requirement that simply and clearly states only what shall be done, making it easy to read and understand. To be concise, the statement does not contain any explanations, rationale, definitions, or descriptions of system use.
- Implementation-free / solution neutral – the requirement states what is required, but not how the requirement needs should be met. The desired result is stated in functional and performance terms, not in terms of a solution set. An exception is interface requirements which are specified in

IRDs. Interface requirements shall provide complete information so that the two sides of the interface may be designed to work as specified when connected to each other.

- Attainable / achievable / feasible – the requirement may be achieved by one or more developed system concepts at a definable cost. This characteristic signifies that adequate research has been performed to show that the requirement may be satisfied and that the technology cost associated with the concept is reasonable within program cost constraints.
- Complete / standalone – the statement is complete and provides sufficient capability.
- Consistent – the requirement does not contradict or duplicate other requirements.
- Traceable – each requirement should be developed in a way that allows traceability back to its source(s). Associated requirements documentation or databases also needs to identify related requirements and requirements that might be impacted by changes to it.
- Unambiguous – each requirement shall have only one interpretation.
- Verifiable / testable – each requirement shall have an identified means by which to verify that it meets the characteristics established above. To be verifiable, a requirement shall be stated in measurable terms.
- Allocatable – all stated requirements are allocated to the lowest level possible within the physical architecture or assigned to an organization.

Characteristics of Aggregate Requirements

Aggregate requirements are a set of requirements for a system or element that specifies its characteristics in totality. Usually, this requirements set is in requirements documents, specifications, or statements of work (SOW). Characteristics of an aggregate requirements set are identical to those of individual requirements, with an enhanced definition of complete and consistent:

- Complete **-** The set of requirements is complete and does not need further amplification. The set of requirements has addressed all categories of requirements and covers all allocations from higher levels. This characteristic addresses the difficulty of identifying requirements that are necessary but are missing from the requirements set. One approach to identify missing requirements is to walk through the Operational Concept and its associated scenarios from start to finish, then walk through the same set of scenarios and ask “what if” questions. This approach usually uncovers a new set of requirements. A second approach is to develop a checklist of topics or areas, such as a specification outline, and verify that requirements exist in each topic area; or, if they do not exist, that there is a good reason for it. A third approach is to check the aggregate requirements set against a higher level document (if one exists) to verify that all allocated requirements have been included in the set.
- Consistent **-** The set of requirements has no individual requirements that are contradictory. Requirements are not duplicated, and the same term is used for the same item in all requirements. This characteristic addresses the problem of identifying unnecessary or conflicting requirements that are inadvertently included in the set. Assigning program-unique identification to each requirement and conducting thorough reviews are ways to eliminate these requirements.

4. Establish Requirements Verification Methods

This activity develops a verification approach for each documented requirement. Verification methods include:

- **Inspection**: the visual verification of a requirement, such as a color, a size, and model number.
- **Analysis**: the mathematical analysis of collected data to verify a requirement
- **Demonstration**: the use of the system itself to verify the expected output, such as a response to an operator input. This is the most commonly used verification technique, and includes simulations modeled on the designed system.

- **Test**: similar to a demonstration except external test equipment is used.

The Traceability and Verification Table is then transformed into a Verification Requirements Traceability Matrix (VRTM). In the FAA, a VRTM is included as a part of every requirements and specification document. A Verification Requirement specifies the strategy or method used to verify each requirement. The VRTM lists the Verification Requirements. The VRTM defines how each requirement is to be verified, the stage in which verification is to occur, and the applicable verification levels. More information about the VRTM is provided in Section 4.7: Verification and Validation.

3.3.1.3 Outputs

The primary outputs from Requirements Development are the requirements and the associated requirements verification methods.

- **Requirements –** Requirements dictate the tasks the system(s) of interest must perform, and how well the system(s) must perform its tasks. The requirements contain the constraint requirements levied on potential solutions. The functional requirements describe what the solution must do to accomplish its goals and objectives and not how it will accomplish them. Performance requirements define the conditions under which each system function is required to perform. Performance requirements include qualitative (how well) and quantitative (how much) measures as well as time lines or periodicity.
- **Requirements Verification Methods –** Each requirement must have an associated verification method. If a requirement cannot be verified, it is not a valid requirement. These verification methods are used by the Validation and Verification Technical Management Process to test and evaluate delivered capabilities against requirements. See Section 4.7: Verification and Validation for more details.

Successful completion of Requirements Development is measured by the acceptable transformation of stakeholder needs into discrete, verifiable, low-level requirements.

3.3.2 Requirements Management Process

Requirements Management is the process of managing and controlling all requirements and associated documentation throughout the entire life cycle of a system. It provides continuity between requirements and other technical program artifacts and ensures traceability from program to enterprise-level requirements. Figure 31 describes the inputs, activities, and outputs of Requirements Management.

Figure 31: Requirements Management Inputs, Activities, Outputs

The Requirements Management process controls all requirements, requirements changes, and traceability between requirements throughout the project lifecycle. It is an iterative process that Manages, documents, and controls the requirements and changes to them in a traceable manner.

Performance of this process is measured and recorded on a regular basis. The following metrics may be used to evaluate process performance:

- Number of changed requirements. This is based on the number of requirements, including both stakeholder-specified and project-derived under active management.

- Cycle time from requirement change initiation to decision
- Cycle time from change decision to baseline incorporation
- Percent of validated requirements to total proposed requirements

3.3.2.1 Develop Requirements Management Plan

Developing a Requirements Management Plan provides the basis for ensuring application of effective and efficient Requirements Management practices throughout a system's lifecycle. The Requirements Management Plan is commonly found in the Systems Engineering Management Plan (SEMP) for the system of interest, but may also be a standalone document.

The Requirements Management Plan details the total effort in managing requirements, which includes identifying and capturing requirements, analyzing and decomposing requirements, and allocating requirements for the project of interest. Requirements Management Plan inputs include the following:

- Internal and external requirements. Internal requirements come from the other SE processes. External inputs come from sources outside of SE
- Component-specific program guidelines
- Program-specific organizational constraints and assumptions to be used in the program
- Program-specific schedule constraints and events
- Top-level conceptual alternatives, functional analyses, design support alternatives, and initial system evaluations
- Technology availability or constraints

The development of the Requirements Management Plan is explained in Section 4: Technical Management.

3.3.2.2 Control Requirements

The systems engineer must control the requirements and characteristics of those requirements for the duration of their lifecycle. The Configuration Management (CM) process provides the techniques for maintaining the necessary controls. See Section 4.4: Configuration Management for more details on the process.

Manage Requirements Change

This activity manages and controls requirements throughout the product's lifecycle, both before and after instituting formal configuration management, by using a defined change process. The configuration management process establishes and maintains requirements baselines both during the requirements analysis process and after formal release of the requirements. The process also identifies and controls all issues and decisions, action items, formal and informal stakeholder or program management desires and directives, and any other real or potential changes to the requirements.

This change process is invoked when a new requirement is identified or a change occurs during any other activity within the Requirements Management process. The activity is a project-wide, approved approach that documents and controls the identified requirement, its' appropriate attributes, its relationship(s) to other requirements, and allocation to the product of functional and/or verification hierarchies. The activity ensures that all involved stakeholders concur with the baselined requirements and any changes. The process controls allocation of requirements between hardware and software.

This process accounts for changes to Government-Furnished Equipment and Contractor-Furnished Equipment safety-critical items that impact development efforts. The process also accounts for changes resulting from the Verification process. That is, if a test or other form of verification determines that a

change in requirements is necessary, the process ensures that the change process is initiated to accomplish that change.

Requirements stability can be measured by comparing the total number of requirements to the number of TBDs in requirements plus the number of requirements that may be subject to change based on how a project progresses. It is recommended that a requirements set is not advanced through the AMS until it becomes “stable”. A requirements set is considered stable when a minimum of 80% of the requirements are stable.

Horizontal and Vertical Integration

In addition to the requirements and their characteristics, horizontal and vertical integration with other systems engineering products must also be maintained. Horizontal integration identifies relationships between systems engineering products at the same level. Because requirements are derived from the Functional Architecture, and are allocated to the Physical Architecture, consistency must be maintained between all three products.

Vertical integration describes how data at a low level is traceable and related to data at a higher level. In the case of requirements, this means that program-level requirements are traceable to and consistent with enterprise-level requirements. Table 12 provides an example of vertical traceability.

Table 12: Example of Vertical Traceability

Mission Service Level	Flow Contingency Management
Element Level	The NAS shall determine demand.
Sub-Element Level	The NAS shall predict future demand.
Sub-System Level (program)	The system *shall* predict traffic demand for each NAS resource.
Component Level (specification)	The system shall use the flight event data to estimate the traffic demand at each monitored airport, sector, fix, and other NAS resources in a user selectable time interval (s) for up to (24) hours minimum in the future.

The Integrated Systems Engineering Framework (ISEF) describes several processes and techniques for establishing and maintaining both horizontal and vertical integration.

3.3.3 Life Cycle Requirements Management

In FAA, requirements sets are contained in a variety of documents. The high-level enterprise requirements are contained in the NAS-RD, while program-level requirements are found in Program Requirements Documents (PRD). A PRD is created and subsequently updated as a program proceeds through the acquisition life cycle and system requirements mature. The evolution of program requirements documentation consists of a preliminary, initial, and final PRD. In the FAA AMS, an approved fPRD is required to obtain a full investment decision. Once the investment decision occurs, the program proceeds to develop system specifications, component specifications, and interface requirements documents.

The system specification requirements are then developed from the functional architecture and final program requirements, and constrained by the fPR-level physical architecture. At any time during the process, the functions and requirements at a higher level may be revisited and reworked as necessary.

3.3.3.1 Requirements Analysis in Concept and Requirements Definition

During the CRD phase, stakeholder needs are translated into program requirements. These high-level requirements are captured in a pPRD. Within the pPRD, no requirement should be written to be solution-specific or that would restrict the search for solutions.

The pPRD has the following characteristics and types of requirements:

- Requirements are implementation-agnostic (i.e., not solution-specific)
- Identifies all constraints or assumptions that bound the potential solution or limit the scope of the alternatives to achieve operational capability
- Identifies high-level reliability, maintainability, and availability (RMA) requirements
- Safety program requirements to ensure the solution is managed for risk and safety
- Applicable system safety standards and orders included
- Identifies quality assurance requirements – should be limited to standards and orders for quality assurance as listed in the Program Requirements Template
- Identifies configuration management (CM) requirements – should be limited to standards and orders for CM as listed in the Program Requirements Template)
- Identifies the types of tests that will verify the solution meets functional and critical performance requirements, and that the human interface is acceptable. Applicable FAA Test Orders and other test guidance documents are identified.
- Identifies land and facility requirements
- Identifies critical operational issues to be assessed during Operational Testing and by the Independent Operational Assessment team. Critical operational issues relate to operational effectiveness and operational suitability; they are not applicable to human resource service acquisition
- Defines high-level maintenance philosophies for hardware and software.

3.3.3.2 Requirements Analysis in Investment Analysis

During Initial Investment Analysis, the pPRD is evaluated and evolves into an initial PRD (iPRD). The iPRD contains requirements conforming to the preferred alternative, is not solution-specific and supports the Initial Investment Decision (IID). The iPRD exhibits the following characteristics and information:

- Requirements and functions are described with more detail than in the pPRD. The requirements will take into account any derived requirements and allocation of the requirements set based upon the preferred solution.
- RMA values as derived from pPRD values are given more specificity
- Specific safety requirements are included as they are identified in safety assessments and when they become known
- More specific quality assurance requirements are identified as they become known
- More specific CM requirements are identified as they become known
- Critical operational issues are expanded
- The high level maintenance philosophy remains unchanged, unless it changes prior to final investment decision
- System states and modes are defined

As the program progresses towards Final Investment Decision (FID), the iPRD develops into the final PRD (fPRD). The fPRD should include additional requirements as more information becomes available on

the selected solution at IID. The fPRD establishes the baseline program requirements at FID. The fPRD should include the following information:

- The total number of units or scope of services that will be needed to meet the mission need
- Specific RMA values as derived from iPRD values. RMA values should be determined during or after IA and the alternatives selection process
- Requirements for real estate, facility space to accommodate systems, auxiliary equipment, and personnel for end-state operations and transition to the new capability
- Additional specific safety requirements should be included as they are identified in safety assessments and when they become known
- Identifies more specific quality assurance (QA) requirements
- More specific CM requirements should be identified as they become known
- Testing requirements should be expanded to include specific performance evaluation, operational verification, Human System Interface (HSI), and acceptance criteria for the new capability.
- Critical operational issues should be expanded
- The high-level maintenance philosophy should remain unchanged, unless it changes prior to final investment decision
- Represents a stable requirements set. This is determined when the critical requirements are no longer changing. Additionally, the entire requirements set must be stable, using the metric determined at the start of the requirements development process. It is recommended that at least 80% of the entire requirements set are stable, with no changes, for the last quarter before finalizing the document and requesting FID.

3.3.3.3 Requirements Analysis in Solution Implementation

The goal of Solution Implementation is to field a system that satisfies program- and specification-level requirements. Per FAA's Acquisition Management System, the System Specification is a crucial contract document. Hardware/software partitioning cannot be done effectively unless the specification is reasonably complete. For software-intensive systems, it is essential to establish system requirements at the functional level before they are allocated to hardware or software. This is accomplished when the Service Team translates requirements in the Program Requirements Document into a System Specification that governs what the prime contractor will provide. Involvement of the user in this process is essential. These are the types of specification documents:

a) System Specification (Type A) – The System Specification (Type A) is the most important engineering specification document. It defines the system requirements and includes the results from the needs analysis, feasibility analysis, top-level functional analysis, and the CPRs. It allocates requirements to functional areas, and it defines the various functional-area interfaces. This top-level specification leads to one or more subordinate specifications covering applicable subsystems, configuration items, equipment, software, and other system components. Although the individual specifications for a given program may assume a different set of designations, a generic approach is used here.

The Type A specification is the FAA-E specification described in FAA-STD-067. This type provides the technical baseline for the system as an entity, is written in performance related terms, and describes design requirements, including the functions that the system is to perform and the associated metrics. It is placed under configuration management at completion of the System Requirements Review, before issuance of the system Screening Information Request. Type A is the requirements document that FAA uses to procure most systems.

b) Development Specification (Type B) – The Type B specification includes the technical requirements for any item below the system level where research, design, and development are accomplished. This may cover an equipment item, assembly, computer program, facility, or

critical support item. Each specification includes the performance, effectiveness, and support characteristics that are required in evolving design from the system level downward.

A system vendor usually produces the Type B specification in response to the FAA-developed System Specification. It is placed under configuration management at completion of the Preliminary Design Review (PDR).

c) **Product Specification (Type C) –** Type C includes the technical requirements for any item below the top system level that is currently in the FAA's inventory and may be procured off-the-shelf. This may cover standard system components (e.g., equipment, assemblies, units, and cables), a specific computer program, a spare part, or a tool. A system vendor usually produces the Product Specification in response to the FAA-developed System Specification or to a vendor-developed Development Specification. It is placed under configuration management at completion of the Critical Design Review (CDR).

3.3.3.4 Requirements Analysis in In-Service Management

Requirements for monitoring, assessing, and optimizing the performance of a capability during its in-service lifecycle are documented in the fPRD. These requirements are used to determine if the new capability is working as intended in the operational environment. The requirements also assist in determining the capacity of deployed assets to meet any emerging demand for services so that a replacement or upgraded capabilities can be obtained and deployed when needed.

FAA conducts a Post Implementation Review (PIR) between 6 and 24 months after the first product of an investment program has become operational. PIR exception reports provide the agency with useful information and recommendations on how best to satisfy unfulfilled requirements, needs, and performance either with the current program or by other means.

3.3.4 Special Considerations for Requirements Analysis

3.3.4.1 Critical Performance Requirements

Critical Performance Requirements (CPR) represent attributes or characteristics considered essential to meeting the needs that the program is seeking to satisfy. CPRs are part of the total program requirements that define the performance baseline for the investment. CPR values are expressed as units of measure. The value represents the acceptable operational values outside of which the utility of the solution becomes questionable. The failure to attain program CPRs may degrade product performance, delay the program and impact dependent programs, or place into question the overall affordability and capability provided by the solution.

The initial CPRs are identified in the iPRD prior to IID, finalized in the fPRD, and included in the Acquisition Program Baseline (APB). CPRs are written as MRSs and included in the iPRD and fPRD.

CPRs must be testable for effective validation and verification (V&V) and decision-making processes. Summarize the CPRs in a manner similar to Table 13.

Table 13: Sample CPR Summary Table

Critical Performance Requirements	
Performance Requirement	**Value (unit)**
Requirement 1	
Requirement 2	
Requirement N	

Initial CPRs are identified in the iPRD prior to the initial investment decision, finalized in the fPRD, and included verbatim in the acquisition program baseline. For programs, the service organization with the mission need

must write each critical performance requirement as a mature requirements statement (MRS) in appropriate sections of the Program Requirements Document using their values in the statement. The service organization with the mission need is responsible for identifying and documenting meaningful critical performance requirements that are central to meeting the intended mission need and benefit targets in the business case.

Management of Critical Performance Requirements

Critical performance requirement status provides the decision authority with pertinent information regarding a solution's progress toward operational acceptability. At milestone decisions, validated and verified critical performance requirements justify approvals for proceeding into:

1. Solution implementation
2. System production
3. Initial operational use
4. In-service management

During program reviews, the status of critical performance requirement provides the decision authority with insight into program progress towards its end state. This status information is used to identify program risks and issues, allowing opportunities to make adjustments to underperforming programs. The decision authority should ensure the total number of critical performance requirements is the minimum number required to characterize what is needed to meet the mission need. During development of the program requirements document, performance requirements that do not support achievement of critical performance requirement values are part of the engineering trade space.

Critical performance requirements also provide additional attention and priority during the conduct and reporting of test and evaluation so as to evaluate the ability of the system or service to fulfill the mission. Planning for early and formal test should give precedence to critical performance requirements over other requirements. Test and evaluation results roll up detailed test and evaluation data based on critical performance requirements to assess overall performance and limitations of the system or service to better support decision-making and risk management.

3.3.4.2 Considerations for System of Systems

In a System of Systems (SoS) environment, requirements that are necessary for fulfilling an investment's business case may be satisfied by another system. In this case, it can be necessary to distribute requirements across multiple investments.

Given the complexity and interconnectivity of the SoS within the FAA, a program's success may rely on certain functionalities being provided by other programs. When developing and managing requirements for an individual system, the engineer must also consider how requirements at the SoS level are affected. Complete requirements management includes managing requirements for the system of interest along with all dependent systems.

For example, consider an enterprise-level requirement to display data with a certain level or accuracy. In order to realize that requirement, the data source must first acquire that data within that level or accuracy. Next, a processor might have to format the data while maintaining that level of fidelity. Finally, the display system must be able to present the information at a high enough accuracy to meet the requirement.

Additionally, when managing future requirements, the engineer must consider traceability and correlation between the desired capabilities and the configuration of the SoS in the given timeframes. In the above example, an improved display system would provide little benefit until the data source was complete.

Considering dependencies between systems over time can help to influence budgetary and technical decisions.

Each sub-system that is acquired through separate investments, but relies on other investments, must maintain the distributed requirements necessary to meet the enterprise level requirement. Figure 32 shows how concepts from the enterprise level flow down and are distributed across investments.

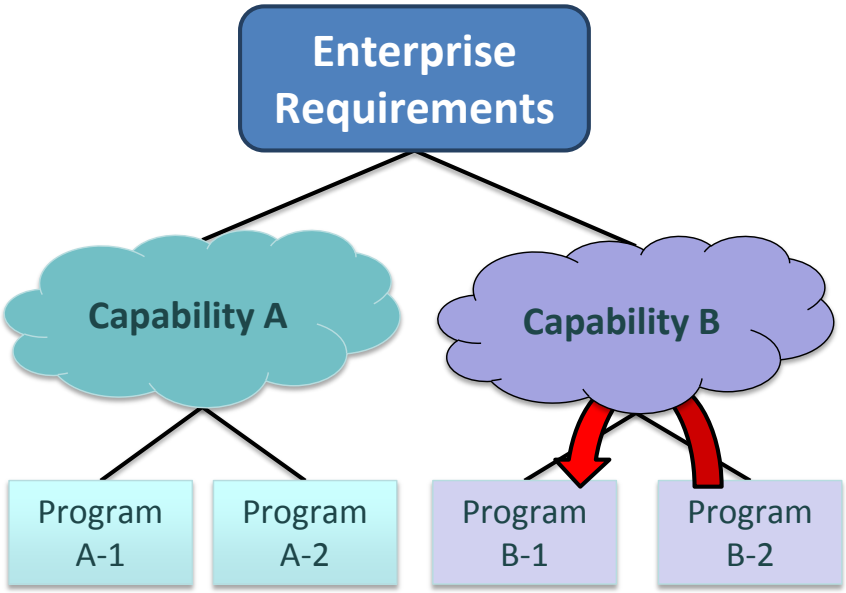


Figure 32: Enterprise Requirements Distribution

In the FAA, SoS requirements must be documented at the program level and/or the specification level for each investment involved. In the example shown in Figure 32, if Program B-2 is reliant on requirements from Program B-1, and those requirements have been allocated from the Enterprise, the SoS requirements must appear in the documentation for both programs. The documentation must also describe the source of the SoS requirement, or where it has been allocated to.

Managing SoS requirements is challenging due to the fact that each involved investment is likely to be at a different level of maturity within the AMS management lifecycle. Accurate documentation, traceability, and configuration management are essential; these tasks can be greatly assisted through the use of an automated requirements management tool.

3.3.4.3 Requirements Management Tools

There are a variety of mechanisms that can help organize requirements and their related information. Deciding which one to use depends on a variety of factors, including the size and complexity of the project, the number of requirements, and the budget. It is highly recommended that a secure and adaptable data repository or database be used to store, track, identify, and allow changes; to rank the changes; and to filter requirements and their traceable elements. Source documents and linkages to artifacts should also be maintained in the same database relative to the requirements.

The FAA standard software tool for requirements management is the Dynamic Object Orientation Requirements System (DOORS), from IBM Rational. This tool helps to ensure proper Configuration Management and requirement traceability. If a prime contractor uses a different Requirements Management tool, it is recommended that the tool have the following core capabilities:

- **Requirements Documentation** – storing requirements, status, requirement type, rationale, and history (version control); presenting the requirements in a user-defined format

- **Traceability** – linking requirements to their parent, child, and peer requirements; providing user-defined, requirements traceability matrices
- **Allocation** – linking requirements to the product hierarchy; enabling user-defined, requirements-allocation documentation
- **Verification** – linking requirements to specific verification approach attributes; enabling requirements verification and compliance documentation
- **Traceability Impact Assessment** – assessing the impact of proposed changes to the requirement, product, and verification hierarchies
- **Compatibility** – communicating with other automated tools, as required.

Additional Information

For sources of information used to generate content throughout this section, see References.

To learn more about the topics in this section, see Additional Tools and Reading Recommendations.

3.4 Architectural Design Synthesis

Architectural Design Synthesis identifies viable design alternatives, refines those alternatives to satisfy program requirements, and ultimately selects the most balanced and beneficial architecture design. Requirements Analysis (Section 3.3) and Functional Analysis (Section 3.2) are tightly coupled precursor SE processes. After multiple iterations, these two processes produce outputs which serve as the primary inputs to Architectural Design Synthesis.

Architectural Design Synthesis transforms requirements – as set in context by the functional architecture – into a design or physical architecture that describes an arrangement of system elements, their interfaces, and the design constraints. An analysis of alternatives then selects the preferred solution based on factors such as cost, schedule, performance, and risk.

Architecture Design Synthesis results in a solution architecture comprised of system elements, their characteristics, and arrangement, that meets the following criteria:

- Satisfies the requirements
- Implements the functional architecture within the constraints of the to-be enterprise architecture
- Is close to the true optimum within the constraints of time, budget, available knowledge and skills, and other resources
- Is consistent with the technical maturity and acceptable levels of risk

Figure 33 is an overview of the process and its inputs and outputs.

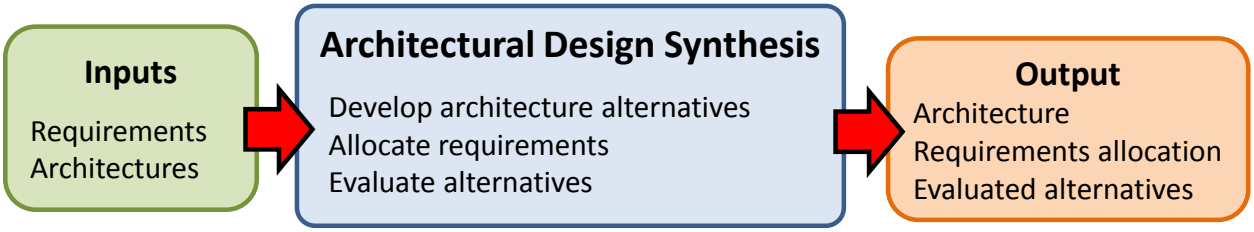


Figure 33: Architectural Design Synthesis Inputs, Tasks, and Outputs

3.4.1 Inputs

The primary inputs to Architectural Design Synthesis are various forms of r*equirements* and a*rchitectures*.

Requirements

The requirements used as inputs to Architectural Design Synthesis will vary depending on the life cycle phase of the project. The Requirements Analysis process iteratively identifies and refines top-level requirements to successively lower levels which then provide the requirements for Architectural Design Synthesis.

Program requirements dictate the tasks the system(s) under design must perform through functional requirements, and how well the system(s) must perform its tasks through documented performance requirements. Program requirements ensure system compliance, function, and performance through measurable verification requirements. The program requirements contain the constraint requirements levied on potential solutions. The functional requirements describe what the solution must do to accomplish its goals and objectives and not how it will accomplish them. Performance requirements define the conditions under which each system function is required to perform. Performance requirements include qualitative (how well) and quantitative (how much) measures as well as time lines or periodicity.

Constraints further limit the system under design from reaching its desired level of achievement. System design usually faces limitations; therefore, design constraints must be identified, documented, and managed so that they do not manage design by default.

Architecture

During Functional Analysis (Section 3.2), the high-level functions are decomposed to lower level functional groups that can be satisfied by system design alternatives. The functional architecture is a hierarchical arrangement of functions and interfaces that represents the complete system. Functional Analysis provides the appropriate area of the functional architecture at which to begin the design process.

The existing approved enterprise architecture is also part of the architecture input. The architecture being developed by the program needs to trace vertically to the enterprise-level operational views (OV) and system views (SV). The enterprise-level technical views (TV) provide FAA standards, guidance, and constraints on how the program level architecture is built. The Integrated Dictionary (AV-2) provides a starting point for the architecture by defining existing architecture entities that can be reused in the architecture being developed. The roadmaps provide information on which existing architectures are linked to or tasked to provide functionality to the "to be" developed architecture. The enterprise architecture products can be obtained from the NAS EA Portal or the Chief Enterprise Architect (CEA) for IT investments.

Appropriate architecture components from the tasked or linked architectures need to be part of the architecture input. The Overview and Summary Information (AV-1) can be valuable in describing the planned linkages to the architecture you are building. The SVs will describe the linked architectures functions and how the architect interfaces with the rest of the enterprise. These architect products are used to ensure horizontal integration and provide guidance in developing the architecture.

3.4.2 Process Components

Architectural Design Synthesis involves selecting a preferred solution or arrangement from a set of alternatives and understanding associated cost, schedule, performance, and risk implications. It entails undertaking a number of distinct steps to achieve measurable goals and objectives while striving to manage or overcome constraints. There are three main activities needed to accomplish Architectural Design Synthesis:

- Develop Architecture Alternatives
- Allocate Requirements
- Evaluate Alternatives

The three activities are iterative and may occur in parallel.

3.4.2.1 Develop Architecture Alternatives

Architecture Design Synthesis begins with a review of the requirements, enterprise architecture products, and functional architecture in order to understand what is to be performed and at what level of performance to meet stakeholder needs. Establishing objectives assists in optimizing adherence to the requirements set within the constraints imposed on the design process. Objectives take into consideration include operational criteria, mission success, technical performance, cost, schedule, quality, risk, failure rate, maintainability, and supportability. Definition and prioritization of all design solution objectives assists in developing architecture solutions that satisfy the requirements. Design alternatives arise from identifying the following items:

- Technology requirements: address the potential incorporation of existing technology into design solutions, in addition to the risks and limits imposed by (and on) that technology. The potential benefits of inserting the technology must outweigh the potential risks to cost, schedule, and performance.
- Specialty Engineering attributes: identify the characteristics of each potential architecture alternative necessary to fulfill interdisciplinary needs.

- Existing systems, applications, service components and tools, such as database or document management systems and technologies in the EA that can provide some or all of the requirements,
- COTS opportunities: evaluate each alternative to determine if a COTS item exists that will fulfill the allocated requirements.
- Make-or-buy alternatives: cost, security, and risk analyses are performed for the architecture alternatives to support a make-or-buy decision. These analyses should address whether it is more cost-effective to produce the design from existing applications or EA components, build it as a new system, or use an established COTS or systems development seller.

Architectural Design Synthesis Inputs

Architectural Design Synthesis can commence once inputs are available; these are typically the outputs of other SE processes, as shown in Figure 34. As part of an iterative solution-development cycle, Architectural Design Synthesis may create or update requirements and architecture products that need to be looped back to Functional Analysis (the "design loop") and Requirements Analysis ("requirements verification loop") for further refinement. In this manner, a set of viable solution alternatives is developed that meets stakeholder needs and satisfies operational shortfalls.

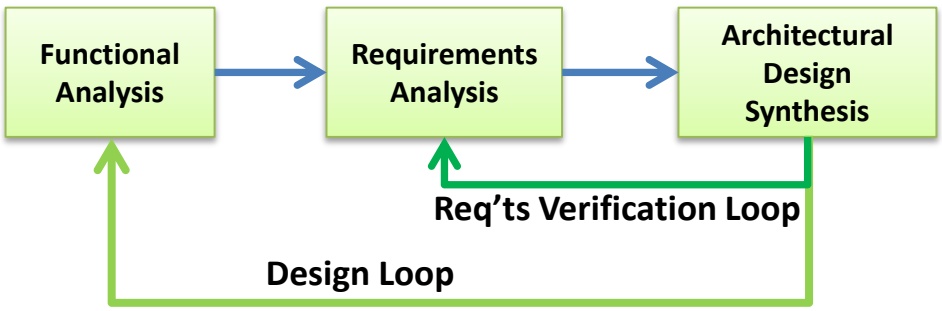


Figure 34: Iteration of SE Processes

Table 14 lists the many types of information that may be inputs to Architectural Design Synthesis. It also indicates the processes that create or deliver the information. Note that not every input is available during the first iteration. For example, market research, trade studies, and risk mitigation plans are often developed later in the process.

Table 14: Needed Architectural Design Synthesis Data

Input	Delivering Process	SEM Section
Program Requirements	Requirements Analysis	3.3
Functional Architecture	Functional Analysis	3.2
Legacy System Specifications	External to SE	
Legacy Interface Requirements	Interface Management	4.2

Input	Delivering Process	SEM Section
Draft ISPD	Integrated Technical Management	4.1
Operational Services and Environment Description	Functional Analysis	3.2
Preliminary WBS	Integrated Technical Management	4.1
Market Research	External to SE	
Trade Study Report	Decision Analysis	4.6
Risk Mitigation Plans	Risk Management	4.3

The objective of developing alternative architecture solutions is have several options from which a final solution architecture will be selected or evolve. Architecture alternatives are developed as data becomes available during the iterative synthesis loops. Ideally, the chosen architecture should satisfy all requirements, but it is useful to include solutions that challenge the requirements and may lead to a better system concept via iteration. Additionally, it is possible that no single architecture design satisfies all the requirements associated with the service gap being addressed. NAS and NextGen architectures being developed are documented using views defined in the Integrated Systems Engineering Framework (ISEF). IT investments utilize the Federal Enterprise Architecture Framework (FEAF). These frameworks provide guidance on what architecture products are required depending on where the design synthesis is in the acquisition lifecycle.

Architecture Views

The ISEF and FEAF describe the baseline set of views required for “As Is” and “To Be” architecture development. Tailoring of the required views can be requested based on the individual and unique needs and aspects of an individual Architectural Design Synthesis. The ISEF guidance does not preclude the development of other DoDAF views that maybe necessary to flush-out the architecture. In addition, the NAS Chief Architect may deem other views as necessary or desired.

The architecture views of the ISEF are based on the Department of Defense Architecture Framework (DoDAF). It allows elements, attributes, and entire architecture views to be customized for a given project. The FAA-required EA products can be found in the ISEF, via the NAS EA Portal. The common architecture products (e.g., OV-1, SV-2) are usually developed in the order shown in Figure 35. Some programs have limits on personnel and time available to do architecture work and might not produce all of the products shown, while other programs may develop additional architecture products.

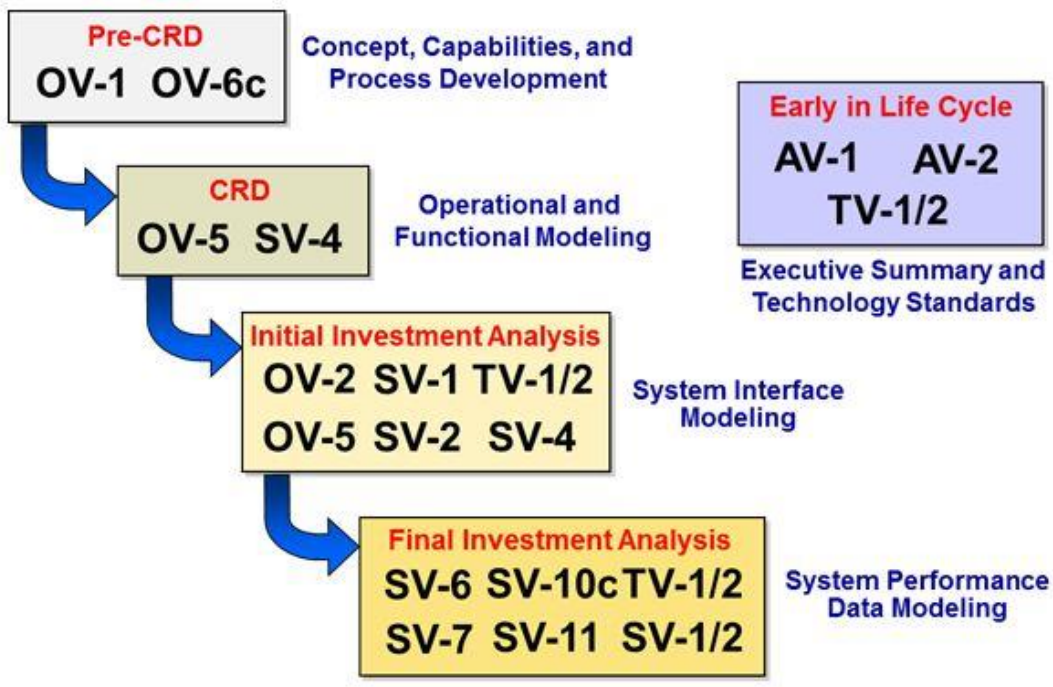


Figure 35: Architecture Product Development

The following is a description of commonly developed architecture products:

- The **Overview and Summary Information (AV-1)** provides consistent executive-level summary information that you can use as a quick reference and to compare architectures and their sub-architectures. The AV-1 includes assumptions, constraints, and limitations that may affect high-level decision processes involving the architecture of interest.
- The **Integrated Dictionary (AV-2)** contains definitions of terms used in the given architecture. It consists of a glossary, a repository of architecture data, their taxonomies, and their metadata (i.e., data about architecture data), including metadata for tailored products associated with the architecture products developed. Metadata are the architecture data types, possibly expressed in the form of a physical schema.
- The **High-Level Operational Concept Diagram (OV-1)** provides a graphical overview of the system depicted in its intended operational environment. The OV-1 is a technical vision for the system end state and the systems engineer frequently must work with a graphical artist to produce an effective OV-1. The diagram is accompanied with some descriptive text.
- In the NAS, the **Operational Node Connectivity Description (OV-2)** is primarily an Enterprise-level product. Operational Nodes are defined as physical locations where actors/performers reside and conduct operational activities.
- The **Operational Information Exchange Matrix (OV-3)** identifies information elements and relevant attributes of the information exchange and associates the exchange to the producing, and consuming operational nodes and activities and to the need-line that the exchange satisfies. In the NAS, the OV-3 is primarily an Enterprise-level product. This product is modified to form a hybrid with the System Data Exchange Matrix (SV-6) elements and attributes to create a special NAS EA OV-3.
- The **Operational Activity Model (OV-5)** describes the operations that are conducting in meeting a business or mission goal. Typically OV-5 products are based on the Integration Definition for Function Modeling (IDEF0) methodology. However, since there are other methods to build OV-5

products, such as Business Process Modeling Notation and Unified Modeling Language swim lane methods.

- The **Operational Event/Trace Description (OV-6c)** is used to describe operational activity sequence and timing that traces the actions in a scenario or critical sequence of events.
- The **Logical Data Model (OV-7)** is strictly an Enterprise-level product for the NAS. This product is used to form the logical starting point for Program-level SV-11 Physical Schemas.
- The **Systems Interface Description (SV-1)** is a critical architecture product for most programs because it documents the required interfaces between system nodes and interfaces between systems. The Enterprise-level SV-1 describes the NAS systems, services, interfaces, and allocated functionality.
- The **Systems/Services Communications Description (SV-2)** describes the data mechanism used to execute systems interfaces. This product focuses on establishing boundaries and depicting communication implementation approaches between the NAS and various stakeholder systems.
- The **Systems Functionality *(SV*-4)** documents system functional hierarchies and system functions as well as the data flows between the system functions. The Enterprise-level SV-4 is represented as a “taxonomic functional hierarchy” rather than a set of data flow diagrams. A taxonomic functional hierarchy helps to visualize the evolution of the NAS towards a service oriented paradigm where services are reused across the enterprise as opposed to individual investments implementing all functions as a standalone capability. This is particularly useful in capability-based procurement in which it is necessary to model the functions that are associated with particular capability. For Service Unit and Program-level architectures, SV-4 is represented by Data Flow Diagrams. In addition, the Enterprise-level SV-4 is the structure by which the NAS requirements are aligned.
- The **Operational Activity to System/Service Function Traceability Matrix (SV-5)** is the enterprise-wide mapping of the operational activities to the system/services sub-functions, therefore identifying the transformation of an operational need into a purposeful action performed by a system or service.
- The **Technical Standards Profile and Forecast (TV-1/2)** lists the rules, standards and conventions to be used by systems and services to implement the NextGen architecture. The TV-1/2 spans all time frames and therefore will appear in the As-Is, Mid-Term, and Far-Term sections of the NAS EA Browser

The EA tool, System Architect (SA), provides queries to find applications, technologies, data and associated performance criteria for business capabilities and associated processes that enable understanding how all of these dimensions of a system.

3.4.2.2 Allocate Requirements

This step furthers the design process by allocating the existing requirements to the system elements (systems, functions, personnel, or support activity components, and/or appropriate organizational entities). Allocation of requirements to elements is an iterative process that occurs when it is determined that the functional element can be accomplished by existing or newly developed items. If the functional element requires decomposition to permit its allocation, functional analysis is performed to partition the functional element sufficiently to permit its allocation among hardware, software, and humans.

All requirements must be allocated. Subsequent analyses, requirement decomposition, and trade studies may produce additional requirements that define the most balanced requirements allocation for the product. Requirements traceability is established and recorded to ensure that all functions are allocated to elements of the system.

Initial allocation in the requirements management process only designates high-level product components, as a complete design should not yet be determined. As the product design matures, the identified requirements may be allocated to lower level components in the physical architecture such as

hardware and software configuration items. Allocation may be continued beyond this level depending on program needs. Requirements may also be allocated to incremental allocated baselines. The process establishes functional, performance, and verification requirements for each incremental system or software version.

Requirements Allocation Matrix

Technical requirements are allocated to the physical architecture defined during the Design Solution Process via the Requirements Allocation Matrix (RAM). The RAM establishes and maintains two-way traceability between the design as depicted in the physical architecture, and the requirements, and between the requirements and the functional architecture. This facilitates the two-way requirements traceability from system specification to hardware and software configuration item specifications. Table 15 is an example of a RAM, which contains the following minimum data:

- The Function ID from the Functional Architecture
- The Function Name
- The requirement that was derived from the function
- The component of the physical architecture that will implement the requirement

Table 15: Requirement Allocation Matrix

Requirement Allocation Matrix			
Functional Architecture		Requirement	Physical Architecture
ID	Name		

Additional information about the requirement and allocation may also be included in the RAM. The RAM will be expanded in the Validation and Verification processes to define validation characteristics and to describe requirements verification methodology.

When a system-level requirement is allocated to more than one configuration item, the process is used to ensure that the lower-level requirements, when taken together, satisfy the system-level requirement.

3.4.2.3 Evaluate Alternatives

As architectural designs are refined, each alternative is evaluated to determine how well it satisfies requirements and constraints and how it adds to the overall effectiveness of the system, a higher level system or SoS. This evaluation includes:

- Ensuring that design constraints are taken into account in the design;
- Assessing and communicating the emergence of adverse system properties resulting from the interaction of candidate system elements or from changes in a system element;
- Performing effectiveness assessments, trade-off analyses and risk analyses that contribute to a feasible, effective, and stable design.

Models and/or prototypes may be developed to assist in:

- Identifying and reducing risks associated with integrating available or emerging technologies
- Verifying that the architecture design solution meets allocated functional and performance requirements, interface requirements, workload limitations, and constraints

- Verifying that the design solution satisfies functional architecture and program requirements

Each architecture design is analyzed to determine how it satisfies the allocated functional and performance requirements, interface requirements, and design constraints. The architecture is analyzed regarding its capacity to evolve, accommodate new technologies, enhance performance, increase functionality, or incorporate other improvements once the system is in production or in the field.

If none of the architecture alternatives achieve full requirements compliance, and all fail to meet the same requirements, a design loop ("iteration") is initiated. The design loop involves revisiting the functional architecture to verify that the physical architecture developed is consistent with the functional and performance requirements. If some, but not all, of the alternatives fail to fully meet all of the requirements, and compliance varies among approaches, the requirements feedback loop is initiated for each design. The system design is audited to determine compliance with the program requirements set. Audits are performed at various levels to assess compliance with requirements. Audit results are then fed back to earlier Architectural Design Synthesis steps as needed.

Architecture alternatives are evaluated to ensure integration with other architectures. Each alternative should be vertically integrated with the enterprise architecture. If there were architectures identified that are linked to the architecture being developed, the horizontal integration with those architectures needs to be documented. The ISEF provides guidance on how to conduct both vertical and horizontal integration.

The preferred architecture is selected by using all prior analyses conducted in Architectural Design Synthesis in conjunction with Requirements Management, Functional Analysis, Specialty Engineering, and Risk Management. The designation and description of interfaces among design elements are finalized, and the architecture is baselined and placed under formal configuration management. Elements, their arrangement, the interactions among elements, and description of the system's features and parameter values characterize the system's architecture baseline.

The selected design solution is specified in terms of its functions, performance, behavior, interfaces and implementation constraints. These specifications form a significant part of the actual system solution. They may be in the form of top-level specifications, sketches, drawings or other descriptions appropriate to the maturity of the development effort. They also serve as criteria when deciding whether to produce, re-use, or acquire each of the identified system elements.

3.4.3 Outputs

Due to Architectural Design Synthesis being an iterative process, the degree of detail of the outputs will vary depending on the position of the project in the AMS lifecycle. Prior to selection of the "best value" alternative, outputs are completed concisely and at a high level for all architecture alternatives. As the functional architecture and requirements continue to be refined there will be fewer architecture designs that fulfill stakeholder needs. As the process narrows towards the selected alternative, the top choice shall have detailed, documented outputs from Architectural Design Synthesis.

The following Architectural Design Synthesis outputs occur throughout the iterations, but vary in scope and detail based on the project's position within the AMS cycle:

- Solution architectures
- Updates to Enterprise Architecture (if needed)
- Description of Alternatives
- Requirements Allocation
- Constraints

Solution Architecture

For all alternative architecture solutions, the system elements are identified along with their arrangement and interactions between them. The architecture is established at a level that documents the design solution and interfaces. It includes requirements traceability and allocation matrices, which capture the allocation of functional and performance requirements among the system elements. Physical architecture

definitions are documented, along with trade-off analysis results, design rationale, and key decisions to provide traceability of requirements up and down the architecture. Verification of the design architecture must be accomplished to demonstrate that the architecture satisfies both the validated requirements baseline and the verified functional architecture. If an alternative requires a modification to NAS or FAA EA data, Infrastructure, Application, or Security Reference Models, then the modifications, costs, and risks associated with the modifications must be documented and reported as part of alternatives analysis and be explicit if part of the recommended solution architecture. This information is further compiled into a Requirements Compliance Matrix.

Description of Alternatives

A separate description for each of the architecture alternatives developed and refined during Architectural Design Synthesis is documented. For the selected architecture, more detail is provided to enable other SE processes to best use the information.

Requirements Allocation

All requirements have been mapped to system elements. As the mapping occurred during Architectural Design Synthesis, a matrix was developed containing all requirements, the elements to which they were assigned, and the level of adherence to the requirements achieved by the system component. The matrix is designed for each level of the physical architecture and it lists all performance, functional, and constraint requirements to reflect each level of the architecture. The system requirements and design constraints are transformed into appropriate component specifications in accordance with the identified physical architecture. The qualification section of individual specifications should identify the methods that will be used to confirm that each component specification has been satisfied under normal and abnormal condition (IEEE 1220 2005).

The Interface Specifications denote the physical interfaces among products, subsystems, humans, lifecycle processes, and external interfaces to interacting systems. The specifications to control the interfaces are documented in Interface Control Documents (ICD).

Constraints

Architecture Design Synthesis looks at many different aspects of the system design, including cost, scheduling, feasibility, requirements, function, and others. As various solutions are considered and refined, constraints become apparent.

Design constraints are documented and sent for further study during Lifecycle Engineering, aiding in identifying the timing of future replacement schedules.

3.4.4 Life Cycle Architectural Design Synthesis

After ensuring that all needed available synthesis data has been gathered, Architectural Design Synthesis begins with a review of the program requirements and the functional architecture in order to understand what is to be performed and at what level of performance to meet stakeholder needs. If it is the first-time entry into Architectural Design Synthesis, or the first synthesis loop, not all data will be available.

Once initiated, Architectural Design Synthesis is generally an iterative process that loops back through Requirements Analysis and Functional Analysis to further refine the requirements and functional architecture to optimize the potential for viable design alternatives. Starting from the Enterprise Architecture, the initial Functional Analysis produces the functions for the initial Functional Architecture. These functions, along with the performance and nonfunctional requirements, are formed into the first system requirements and documented in the Shortfall Analysis. Architectural Design Synthesis begins once the initial functional architecture is developed and the Mission Need is decomposed.

3.4.4.1 Architectural Design Synthesis during CRD

During CRD, the Functional Architecture is developed as an output of the Functional Analysis process. This is used to refine the Mission Need requirements into the first set of requirements; these are documented in the pPRD.

The first loop of Architectural Design Synthesis is then initiated to translate the Functional Architecture-based requirements into a physical architecture by defining and allocating the system elements. This synthesis step includes generating alternative design solutions that satisfy the Functional Architecture. Market research helps determine available technologies, research needed to mature an emerging technology to serve the solution architecture, or various systems that can meet all or part of the program requirements. If multiple viable alternatives do not exist, the program requirements and Functional Architecture may be modified in concert with the user organization, and iterated as needed.

3.4.4.2 Architectural Design Synthesis during Investment Analysis

During the Initial Investment Analysis, the pPRD evolves into an iPRD. The iPRD contains requirements conforming to the preferred alternative, is not solution specific and supports IID. As the functional architecture and requirements continue to evolve, Architectural Design Synthesis iterates. Synthesis activities strive to identify viable design alternatives, refine those alternatives to fulfill the requirements, and select the most balanced and beneficial design to introduce into the field. The alternatives are reduced to reflect only those alternatives considered viable or worth pursuing. Compliance with the program requirements for the functional area is reviewed and analyzed.

For each alternative, the solution level of compliance to all requirements is documented. If none of the alternatives achieves full compliance, and all fail to meet the same requirements, the design loop is initiated. If some, but not all, of the alternatives fail to fully meet all of the requirements, and compliance varies among approaches, the requirements feedback loop is initiated for each design.

The “best value” alternative is recommended to the Joint Resource Council (JRC) using all prior analysis conducted as part of Architectural Design Synthesis or in conjunction with Requirements Analysis (Section 3.3), Functional Analysis (Section 3.2), Specialty Engineering (Section 5), and **Error! eference source not found.** (Section 4.3). Upon being approved at Initial Investment Decision, the solution design is finalized in details along with the designation and description of all interfaces. After approval at Final Investment Decision (FID), the solution design is baselined and placed under formal configuration management.

As the program progresses towards Final Investment Decision (FID), the iPRD develops into the final PRD (fPRD) As this Synthesis step is entered, the program requirements to be satisfied by the recommended solution are established, and this step furthers the design process by allocating the requirements to physical system elements. Design constraints that apply directly to system elements are identified. As the solution is refined, it is analyzed to determine how it satisfies the allocated functional and performance requirements, interface requirements, and design constraints and how it contributes to the overall performance of the system.

3.4.5 Architectural Design Synthesis Process Tools

Along with the definition of design alternatives, it is important to establish the relationship between alternatives at each level of design activity. The following four tools may be used to represent a description of alternatives.

Concept Description Sheets

A separate description for each of the alternatives developed and refined during Synthesis is documented. For the selected or preferred design, more detail is provided to enable other SE processes to best use the information. The description sheets include a complete description of the system, the system operational use, and characteristics.

Architecture Block Diagrams (ABD)

The ABD documents the hierarchical relationship of all system elements. The ABD includes hardware and software elements and their hierarchy, documentation and data, facilities, test equipment, and support.

An external ABD is also to be developed to depict the external elements that affect the selected system. Like the system ABD, the external ABD should include all hardware, software, facilities, personnel, data, and services having a significant effect on the selected system.

Interface Drawings

Drawings are developed for all system physical element interactions as well as for all interactions to external physical elements. The drawings provide a mental picture of interfaces and are the basis by which interface requirements and control documents are developed later under Interface Management (Section 4.2).

Schematic Block Diagrams

A simplified Schematic Block Diagram (SBD) shows the components that may comprise an element and the data that may flow between them. An expanded version is usually developed that displays the detailed functions performed within each component and their interrelationships. For complex systems, this may then be developed into a logic diagram for auditing the schematics produced. This audit is a critical SE function. Interface information should also be embedded into the SBDs, as appropriate. The interface data will form the basis for the interface specifications to be developed at multiple levels of the system hierarchy. An N-squared (N^2) diagram is extremely useful for developing and auditing interfaces at all levels.

If software is an element of the design, it must be determined whether a given function will be accomplished in hardware or software. Computer Software Elements (CSE) should be defined during this step of the process and embedded within the SBDs. Experience shows that it is helpful to first define the top-level HWCI and/or CSCI in which a given software function will reside before defining which candidate CSEs will accomplish the function. Additionally, it is recommended that a given function be tracked to determine whether it has been allocated to a software alternative or a hardware alternative. Determining the appropriate level of the system hierarchy for defining CSEs is largely project dependent.

The products of this step of the SE process are a set of viable system alternatives responsive to the design goals and a series of SBDs depicting how the alternatives interrelate.

Computer-Aided Design

Modern computing hardware and software are used to convert the initial idea for a system into a detailed engineering design. The evolution involves creating geometric system models that are later manipulated, analyzed, and refined.

3.4.6 Special Considerations

System of Systems

As Architectural Design Synthesis is conducted, special consideration must be made for the FAA SoS environment. SoS are consciously designed and engineered from the beginning to be a SoS with shared business enterprise rules (Gideon, Dagli, and Miller 2005.) The systems engineer may perform Architectural Design Synthesis to develop architecture alternatives, determine the best alternative solution for priority mission needs, and develop and field the solution to satisfy the mission needs. In developing and selecting the architecture solution, the systems engineering must also consider the integration of that system to the larger SoS. The solution must be able to operate independently as well as with other systems in the SoS.

To implement a SoS, an integrating software system is required. If all the other component systems already exist, the systems engineer can focus on the design of the integrating software system. Knowledge of the architecture of the component systems might be needed to achieve an effective design.

Industrial Control Systems

The NAS and NextGen air traffic systems are designated as one of 19 US Critical Infrastructures. By definition the NAS is an Industrial Control System and therefore has additional cybersecurity requirements levied upon it. These are addressed as part of the security authorization process for all FAA systems, but must be considered no later than alternatives analysis in IID. Given the long development

cycle, the architect must consult with AIS-300 (System Security Authorization process) for the trends that are likely to be in effect when the system is deployed as well as using the current FAA Security Authorization Handbook and templates for the requirements that apply.

Additional Information

For sources of information used to generate content throughout this section, see References.

To learn more about the topics in this section, see Additional Tools and Reading Recommendations.

3.5 Cross-cutting Technical Methods

In any phase of the project, the FAA systems engineer might benefit from using certain technical methods to determine feasibility, validate, and further define needed functions and requirements. This section describes the use of modeling, simulation, and prototyping to accomplish these goals. These techniques facilitate the development of complex and costly systems.

3.5.1 Modeling and Simulation

Modeling and simulation involves getting information about how something will behave without actually implementing it in its intended operational environment. Modeling and simulation are effective methods for addressing technical risk on a project because they provide additional insight to find and correct problems before implementing a solution. The planned resources anticipated to be spent in development, validation, and operation of the model should be consistent with the expected value of the information obtained using the model. The terms “modeling” and simulation” are sometimes used interchangeably. They are distinct, though in some instances, closely related terms.

Modeling is the application of a standard, rigorous, structured methodology to create and validate a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. In many cases, the representation of an object or phenomena is subsequently used by a simulation.

From the INCOSE SE Handbook, “a model is a mapping of the system-of-interest onto a simpler representation which approximates the behavior of the system-of-interest in selected areas. Models may be used to represent the system under development, the environment in which the system operates, or interactions with enabling systems and interfacing systems.”

Models can be used within most systems life cycle processes, such as the following:

- Requirements Analysis: determine and assess impacts of candidate requirements
- Architectural Design: evaluate candidate options
- Verification: simulate the system’s environment and evaluate test data
- In- service operations: simulate operations in advance of execution for planning and validation

Models can provide visualization to a concept or a problem to be solved. The visualization allows interrelationships and dependencies to be observed and analyzed. Modeling provides the capability to predict characteristics across the spectrum of system attributes throughout its lifecycle.

Simulation is a representation of the system functions or operations. Through simulation complex scenarios can represent system capabilities through numerous implementation variations of a model. These capabilities allow analysis and understanding into how individual system or process elements interact and affect the intended operational environment.

Simulation modeling allows system developers and analysts to predict the performance of existing or proposed systems under different configurations or operating policies. This process greatly reduces the risk of unforeseen bottlenecks, underutilization or overutilization of resources, and failure to meet specified system requirements or user needs. Simulations also are useful in defining system requirements, establishing risk, and testing interfaces. Simulation predictions guide decisions about the system’s design, construction, and operation, or to verify its acceptability.

Simulation can also support training of personnel in ways that would otherwise be cost prohibitive. Simulation based on accurate modeling allows students to practice using complex Air Traffic Control systems at Oklahoma City training center without endangering actual aircraft or adversely impacting operations.

3.5.1.1 Types of Models

“There is no such thing as an inherently good – or inherently bad – model. To assess the quality of a model, you have to take into account for what purpose the model was created and who the target

audience is. Different purposes and different target audiences may require fundamentally different models" (Lankhorst 2009).

Models fall into one of two general categories – representations and simulation models. Representations employ some logical or mathematical rule to convert a set of inputs to corresponding outputs with the same form of dependence as in the represented system, but do not mimic the structure of the system. Validity depends on showing, through analysis or empirical data, that the representation tracks the actual system in the region of concern.

Simulation models, on the other hand, mimic the detailed structure of the simulated system. "They are composed of representations of system elements, connected in the same manner as in the actual system. The validity of a simulation depends on the validity of the representations in it and the faithfulness of its architecture to the actual system. Usually the simulation is run through scenarios in the time domain to simulate the behavior of the real system. An example might be the simulation of a fluid control system made up of representations of the piping, pump, control valve, sensors, control circuit, and the fluid running through the system.

The type of model selected depends on the particular characteristics of the system that are of interest. Generally, it focuses on some subset of the total system characteristics such as timing, process behavior, or various performance measures. Representations and simulations may be made up of one or several of the following types: Physical, Graphical, Mathematical (deterministic), and Statistical.

Physical models exist as tangible, real-world objects which are identical or very similar in the relevant attributes of the actual or proposed system. The physical properties of the model are used to represent the corresponding properties of the system of interest. Examples of physical models include: wind tunnel, test bed, and breadboard/brass board.

Graphical models are a mapping of the relevant attributes of the actual or proposed system onto a graphical entity with analogous attributes. The geometric or topological properties of the graphical entity are used to represent geometric properties, logical relationships, or process features of the system of interest. Examples of graphical models include: functional flow block diagrams (FFBDs), N^2 diagrams, logic trees, blueprints, schematics, and maps. Examples of using N^2 diagrams are shown in Section 3.2: Functional Analysis.

Mathematical (deterministic) models use closed mathematical expressions or numerical methods to convert input data to outputs with the same functional dependence as the actual system. Mathematical equations in closed or open form are constructed to represent the system. The equations are solved using appropriate analytical or numerical methods to obtain a set of formulae or tabular data defining the predicted behavior of the system. Examples of mathematical models include: operational or production throughput analysis, thermal analysis, vibration analysis, load analysis, stress analysis, Eigen value calculations, and linear programming..

Statistical models are used to generate a probability distribution function for expected outcomes, given the input parameters and data. Statistical models are appropriate whenever random phenomena are involved as with reliability estimates, whenever there is uncertainty regarding the inputs such that the input is represented by a probability distribution, or whenever the collective effect of a large number of events may be approximated by a statistical distribution. Examples of statistical models include: Lognormal statistical model, logistical support, path analysis, multiple regression, Chi Squared Automatic Interaction Detection, cluster analysis, discrete and continuous models.

3.5.1.2 Types of Simulations

There are many types of simulations that an engineer can use to predict system behavior. A basic description of each type is included below in the order of increasing complexity and fidelity of the results.

Discrete Event simulations are simulations based on queuing theory. For discrete event simulations the simulation is not continuously updating data but processes the data once a new input is provided to the simulation.

Continuous simulations are simulations that continually provide output data based on a range of inputs. The most common continuous simulation used is a Monte Carlo simulation. A Monte Carlo simulation provides averages and probability distributions. In addition to examining nominal conditions, non-nominal Monte Carlo simulation can establish system reactions or breakage when exposed to extraordinary or unusual conditions.

Agent-Based simulations are simulations that contain several data blocks, called agents. Agents contain a set of instructions to act independently when they encounter other agents or constraints in the simulation. These data blocks are considered to show a basic level of artificial intelligence. Agent-Based simulations are better simulations for predicting human behavior than the previous types of simulations.

Artificial Intelligence simulations combine agents form agent-based simulation with a means of resolving uncertain events. Uncertain events are introduced as models consistent with probability theory and artificial intelligence simulations can utilize several uncertainty resolution techniques, such as Bayesian networks and fuzzy logic.

Game and Virtual World simulations are physical and graphical representations of an operational scenario that is intended to incorporate live people. These simulations are primarily used for training purposes but can also provide an advanced analysis of system operations.

An **optimizing** simulation can use one or all of the previous techniques to provide a quicker way of examining a range of sizes and parameters, as opposed to a single design option. This assists the systems engineer in determining the best solution. Optimization simulations can also help to determine the ideal size and performance characteristics of the proposed system.

3.5.2 Prototyping

Prototyping is a technique that can significantly enhance the likelihood of providing a solution that will meet the user's need. In addition, a prototype can facilitate both the awareness and understanding of user needs and stakeholder requirements. This section briefly discusses two types of prototyping: rapid and traditional.

Rapid prototyping is probably the easiest and one of the fastest ways to get user performance data and evaluate alternate concepts. A rapid prototype is a particular type of simulation quickly assembled using software combined with hardware that presents a menu of existing physical, graphical, or mathematical elements. Examples include tools such as laser lithography, selective laser sintering, computer numerical control machining services, fused deposition modeling, 3D printing, and computer simulation environments. They are frequently used to investigate concept models, design iterations, engineering evaluations, form and fit, human-system interfaces, operations, or production considerations. Rapid prototypes are widely used, but since they use a menu from the tool to approximate the system elements under consideration, they are usually not prototypes of the planned system.

Traditional prototyping involves building something that exactly represents the behavior in whole or part of the planned system. It is a technique that can reduce risk or uncertainty. A partial prototype is used to verify critical elements of the system-of-interest. A full prototype is a complete representation of the system. It must be complete and accurate in the aspects of concern. Objective and quantitative data on performance times and error rates can be obtained from these higher fidelity interactive prototypes.

Usually prototypes are not "the first draft" of production entities. Prototypes are intended to enhance learning and validate concepts. They should be set aside when this purpose is achieved. Once the prototype is functioning, changes will often be made to improve performance or reduce production costs. The production entity may require different behavior.

3.5.3 Use of Cross-cutting Technical Methods across the Life Cycle

The methods of modeling, simulation, and prototyping are similar regardless of where the development team is in the lifecycle. However methods will produce some different or enhanced analysis as the program moves through the lifecycle.

Technical Methods in Service Analysis

For some programs, modeling and simulation can be used to document high-level concepts and help identify shortfalls. Models help in the analysis of potential architecture changes.

Technical Methods in Concept and Requirements Definition (CRD)

The models used in Service Analysis can be enhanced to help the SE finalize the shortfall analysis. Modeling is useful in developing the solution concept of operations and architecture design. Modeling and simulation can be used to evaluate the different proposed alternatives to determine the pros and cons of each approach. It can also help identify potential safety issues in each alternative. Modeling assists in determining high-level requirements and rough cost estimates.

Technical Methods in Investment Analysis

The models used to evaluate and analyze alternatives in CRD can be enhanced to help determine the preferred alternative. Modeling can be useful in defining a business case. Modeling and simulation using various scenarios can be used to determine and validate requirements. Models can help mature the architecture design. Models are useful in identifying risks and safety issues. A prototype can be used to gain a better understanding of user needs and stakeholder requirements. A prototype can also help to demonstrate the feasibility of a concept. Further elaboration of costing models from CRD help to come up with better cost estimates.

Technical Methods in Solution Implementation

Modeling and simulation can simulate operations before the final product is built. Simulation results will refine the design of the system under development. Simulation of the system's environment and evaluating the test results is beneficial in verifying requirements. Prototyping by the vendor provides the development team the ability to demonstrate key functionality of the system under development. Based on the outputs of the prototype, the system can be modified to better support the mission needs. Modeling of key system components can also be useful.

3.5.4 Tools

Standard tools for all types of modeling and simulation are now available commercially. The FAA does not have all of these tools, but does have tools that have a degree of simulation and the ability to link to third-party simulation tools. The FAA tools are:

- **System Architect (SA)™** -- A tool to create architecture products. Business process modeling diagrams provide links to an external simulation product – Witness™. System Architect provides object-oriented and component-based modeling using the Unified Modeling Language (UML). UML is the current, yet still evolving, standard for object-oriented analysis and design of systems. The rapid prototyping tool "Screen Architect" works with SA to create interface prototypes in RTF and HTML formats.
- **CORE™** -- CORE provides systems engineers with a powerful solution for building complex system models with rich connectivity across domains. Supported by a robust simulation engine, CORE provides end-to-end coverage of the system development process from requirements development to Validation and Verification, where it highlights gaps and missing functions.

Additional Information

For sources of information used to generate content throughout this section, see References.

To learn more about the topics in this section, see Additional Tools and Reading Recommendations.

4 Technical Management Disciplines

Technical management disciplines collectively form a holistic management approach that promotes project effectiveness and ensures that all planned and systematic activities associated with those processes fulfill stakeholder needs and are of the highest quality. They are employed to understand, manage, and continuously improve the various systems engineering processes and sub-processes to produce value-added products and services for the stakeholders.

Within the FAA, there are seven technical management disciplines. They are continuously and consistently applied throughout solution development, and may be implemented with as much rigor and formality as needed. The technical management disciplines are:

1. Integrated Technical Management
2. Interface Management
3. Risk Management
4. Configuration Management
5. Systems Engineering Information Management
6. Decision Analysis
7. Verification and Validation

When implementing any kind of change to established processes, the FAA often relies on a variety of standards and models that help guide the updates. These include CMMI, DO-178, DO-278, iCMM, ITIL, ITIM, ISO/IEC 15504, ISO 9001, ISO 14001, and ISO 20000. No matter which model is used, a Quality Management System (QMS) must be in place throughout an FAA project's lifecycle. A QMS directs, measures, controls, and improves products and services. It has defined policies, processes, and procedures for core business functions. While FAA can select the QMS to be used for the government activities related to a project, a contractor is required to satisfy the contract specifications regarding a quality system. In general, the government can require that the contractor have a QMS, but not the specific QMS to be used.

Additional Information

To learn more about the topics in this section, see Additional Tools and Reading Recommendations.

4.1 Integrated Technical Management

Integrated Technical Management is the tactical and strategic means of defining problems, forecasting conditions, and coordinating program elements to maximize program focus on providing superior products and services. The objective is to provide program management sound, repeatable guidance and direction for executing requirements-based programs in a structured manner. It also provides a feedback mechanism to measure or assess progress against a plan, identifies variances, and provides sufficient information for informed decision making on corrective action(s) to be taken.

Planning determines what tasks will be needed to complete a project. At a minimum, a plan contains the tasks to be performed, a schedule, required resources (roles, tools, travel, training, facilities, support services), and responsibility designations. Technical plans may call for tailoring the SE processes to deliver products and services that satisfy the established requirements. Technical reviews and audits are the primary means to monitor adherence to the technical plans.

Integrated Technical Management applies to all programs regardless of size, complexity, or program status. The size, complexity, and stage of the system lifecycle dictate which SE elements need to be supported by more detailed planning documents. The scope of planning changes throughout the lifecycle

to meet program needs. A change to a program with an existing ISPD, SEMP, or other plans requires documentation only to the extent that existing plans don't support the changes.

Integrated Technical Management consists of two primary areas activities. Developing Technical Plans (Section 4.1.3) is self-explanatory. Technical Monitoring and Control (Section 4.1.4) details how to measure and assess project progress, establish milestones, and develop additional procedures that lead to successful project completion.

4.1.1 Inputs

The primary inputs to the Integrated Technical Management Process are:

- **FAA policy** – The specific applicable policies will vary from project to project and affect the plan being developed.
- **Planning Criteria**. Planning Criteria provide constraints and boundaries for the planning activities. Some examples of planning criteria include:
  - Requirements – bounds the Work Breakdown Structure
  - Architecture – provides arrangement of hardware, software, and personnel components along with interfaces depicting the logical and physical definition of the system.
  - Analysis Criteria – ensures credible analysis methods and results
  - Concepts – applies the Concept of Operations that will guide the project
  - Integrated Master Schedule – provides program milestones and associated dates
  - Corporate Strategy and Goals – provides constraints and boundaries to planning
  - Enterprise Architecture – describes the FAA enterprise architecture, of which the NAS Enterprise Architecture is an integral part

4.1.2 Integrated Technical Management Approach

4.1.2.1 Integrated Technical Management Strategy

An Integrated Technical Management strategy ensures successful systems engineering process implementation. It outlines how the various processes will help satisfy mission needs in accordance with agency policy and guidance. Each project includes a tailored ITM strategy that supports each phase of the project lifecycle.

At a minimum, an Integrated Technical Management strategy does the following:

- Identify all stakeholders
- Identify and gather Integrated Technical Management inputs
- Assign roles and responsibilities for Integrated Technical Management process activities
- Define format for Technical planning documents
- Define technical plans needed for project of interest
- Define schedule for Integrated Technical Management process activities and updates
- Define criteria for technical updates and re-planning needs
- Establish communication plan with stakeholder
- Identify planning tool, if applicable

4.1.2.2 Integrated Multidisciplinary Teams

Within Integrated Technical Management, it is important for systems engineers to realize that their role is central to the larger Integrated Multidisciplinary Team (IMT). The IMT includes all stakeholders, decision makers, subject matter experts, domain engineers, and other key personnel that work towards defining the system at any stage in the lifecycle. The IMT is not meant to impose a set team structure or dictate how a team works together; instead, the IMT establishes the means in which the systems engineer can concurrently consider and act upon the needs of everyone involved in the development of the system throughout the system lifecycle. Because of the integrated lifecycle focus maintaining a strong relationship with the IMT is an essential part of being a systems engineer. In order to ensure optimal system design, the systems engineer must act as the catalyst of the IMT by balancing product and process development with technical recommendations, budgetary or financial constraints, specialty engineering inputs, and stakeholder preferences. The IMT can be a formal team as defined by policy such as Capture Teams or can be more informal teams that forms due to the need for proper Integrated Technical Management.

4.1.3 Develop Technical Plans

Integrated Technical Management prepares the technical plans and directs the technical effort for a project. These plans are maintained throughout the project's lifecycle. The Integrated Technical Management strategy is used to direct the process activities.

The following are developed through Integrated Technical Management:

8. Systems Engineering Management Plans (SEMP)
9. Implementation Strategy and Planning Document (ISPD)
10. SEMP subordinate elements
11. Lifecycle Plan

Note: Each program may develop two SEMPs: a Program SEMP and a Contractor's SEMP. Both SEMPs utilize the same steps for development but one is directed towards the earlier lifecycle phases of a program, from the program management perspective; whereas, the other SEMP is the how the contractor manages activities throughout the lifecycle.

4.1.3.1 Systems Engineering Management Plan

The SEMP integrates all SE activities for the project. It ties together all systems engineering elements required to attain project cost, performance, and schedule objectives. It identifies and ensures control of the overall SE process expands upon the ISPD. The preliminary version of the SEMP typically occurs in Initial Investment Analysis, with a completed version released for Final Investment Decision.

For various programmatic reasons, any SE element in the SEMP may require a more detailed standalone plan (e.g., Risk Management Plan, Configuration Management Plan, CRD plan). Each plan must define the tasks and products of the process, assign responsibilities to various sub-processes and personnel, describe the deliverables, and include the schedule for completion of each task and delivery of each product. The planning details for each Plan are in Section 8.3: Appendix C: System Engineering Technical Reviews and Associated Checklists.

4.1.3.1.1 Program Systems Engineering Management Plan

The Program SEMP is the master planning document used by program management to plan, control, conduct, and fully integrate SE activities to achieve program objectives. It should be initiated during Research for Service Analysis (RSA) to help execute the system development by defining the FAA program's organizational structure and interfaces, establishing the responsibilities, authority, and accountability of each stakeholder group. The Program SEMP provides the program's overall technical approach, including SE processes, resources including roles and responsibilities, key technical tasks, activities with dependencies, schedule/milestones, technical risks and mitigations, inputs and outputs with

quality measurements and thresholds, and success criteria. The Program SEMP also establishes output and outcome priorities to guide the acquisition and development processes.

The Program SEMP is summarized in the Implementation Strategy and Planning Document (ISPD).

4.1.3.1.2 Contractor's Systems Engineering Management Plan

The contractor provides the Contractor's SEMP (CSEMP) early in the Solution Implementation phase shortly after the program contract award kickoff briefing. The CSEMP supports project management by describing in detail the contractor's systems engineering activities and responsibilities, so it may be a subset of the Program Management Plan (PMP). The CSEMP normally will not evolve during a long-lived program, but be supplemented by Task Order or Project Management Plans providing tailoring specifics of the general SEMP to a project or large item delivery task. The CSEMP describes the overall technical approach, including systems engineering processes, resources, technical tasks and their dependencies, schedules and milestones, roles and responsibilities, product and service metrics and thresholds, and overall success criteria.

Inputs to a CSEMP include:

- The contractor's (or prime and sub-contractors') SE process descriptions
- Knowledge of the FAA operational / user Service Organization goals and strategies
- Description and understanding of the business case and acquisition strategy for the project, usually found in the ISPD and from data for the operational or user service organization as described on the FAA intranet and the service organization's FAA environment, e.g., ATO, AVS, ARP, AST or AFN
- Identification of detailed program/project requirements in the Statement of Work (SOW) and occasionally expansions such as the appropriate security category Information System Plan (ISP) template and guidance from the current FAA Security Authorization Handbook
- Contract Terms and Conditions
- Any risks, issues or constraints such as those imposed by the NAS or FAA Enterprise Architecture (EA) existing or future infrastructure and Service-Oriented Architecture (SOA)

4.1.3.1.3 Systems Engineering Management Plan Development

The following are generic steps used to develop a SEMP.

1) **Collect Inputs –** SEMP development relies on information from both technical and nontechnical documents produced by the program and other FAA and DoT organizations. Inputs are also gathered from guidance, best practices documents, AMS program baseline documentation, the fPRD, EA and other review findings, Screening Information Requests (SIR), Statements of Work (SOW), Integrated Master Schedules (IMS), and the draft Implementation Strategy and Planning Document (ISPD).

2) **Analyze Inputs –** The SEMP sections are usually provided by FAA SE practitioners or recommended by FAA Offices responsible for the respective SE functions. They use Program Management and operational or user organization staff's historical data and insight to tailor their SE function's processes into activity networks (swim-lane flowcharts and task descriptions), levels of effort and schedules, identify input sources and dependencies, and technical risks and their mitigations. The initial resource estimates applied to the set of SE function plans with some complexity multiplier can be used for the Independent Government Cost Estimate (IGCE) required by Acquisition shared services to let a contract. The tailoring of SE processes by SE practitioners familiar with similar size, duration, complexity and technology programs and projects is important. For example, large and complex system developments demand full SE applications to ensure success, whereas small-scale projects may only need a much reduced scope, effort and schedule process.

3) **Define Activities, Schedule, and Levels of Effort –** After evaluating all functional inputs, determine how to integrate activities. Decisions involve:
   - Tailoring the integration of SE processes to load-level specific resource types
   - Selecting an approach to reduce technical, schedule, or cost risk
   - Determining how project team members interact and communicate to ensure coordinated, collaborative activity performance
   - Identifying the explicit SE responsibilities, accountability, and authority, and the risks and tradeoffs
   - Developing the structure of the comprehensive SE inputs to the IMS (included in the ISPD) for schedule tasks
4) **Baseline –** Submit the SEMP for review and comment, using input from all affected SE processes, enterprise management, and, when appropriate, the stakeholders. The draft may also include contractual SE requirements, such as Contract Data Requirements List (CDRL) or Data Item Descriptions (DID), with which all affected parties shall comply. More information on baselines is available in Section 4.4: Configuration Management.

   Interface with other SE processes – The SEMP interfaces with, and forms a roadmap to, any other SE and engineering specialty standalone plans. The SEMP should contain technical plans for each SE process as applicable. See Section 8.3: Appendix C: System Engineering Technical Reviews and Associated Checklists for more information on developing the SEMP and SE Plans.
5) **Update and Maintain the SEMP –** Throughout the lifecycle of a project, SE monitors program changes, especially to the ISPD. When there is a significant change, the SEMP is updated to reflect approved changes.

There is no prescribed format for the SEMP. It may be a single plan or consist of multiple plans, depending on the project size and complexity. It contains planning for all SE processes that the project requires. At a minimum, the SEMP must include:

- An introduction, stating the project purpose and referencing relevant SE guidance
- Work Breakdown Structure
- Technical Plans

4.1.3.1.4 Work Breakdown Structure

The Work Breakdown Structure (WBS) includes SE-related roles, including qualification levels, estimates of scheduled durations and dependencies for SE tasks or activities that the SE roles perform, and the levels of effort by SE role needed for the tasks. It also contains the activities, staffing and criteria for technical reviews.

The WBS defines the total scope of the project effort. Each lower WBS level represents an increasingly detailed definition of SE work for a project component. Project components may be projects, tasks, or activities.

The WBS provides the framework for organizing and managing work. It entails breaking the projects into progressively smaller pieces until they are a collection of discretely-defined work packages. The assumption of WBS is that a “waterfall” development approach is valid; this is almost never true, so the WBS is the major evolving part of the SEMP. A well-developed WBS should be at least three to four levels deep, with each level five to nine elements broad.

4.1.3.2 Technical Plans

Each SE process may have a plan – these are summarized in Table 16. Each plan must include a definition of the products and assign responsibilities to various sub-processes, deliverables, and schedules for completion of tasks and delivery of each product. See Section 8.3: Appendix C: System

Engineering Technical Reviews and Associated Checklists for more information on developing the following SE Plans typically contained the SEMP.

Table 16: Listing of Technical Plans

Plan	Scope
Requirements Management Plan	Describes the inputs, activities, methods, outputs, validation and verification mechanisms and criteria, roles and responsibilities, and how to control changes in solution requirements. Also includes the Requirements Traceability Matrix mapping requirements to and from solution architectures, component designs, solution components, user documentation, training materials and test plans
Decision Analysis Plan	Documents assessment of alternative solutions, designs, implementations, documentation, logistics, operations and maintenance issues and risk. May include the same for cost, schedule, issues, and risks.
Interface Management Plan	Documents the interfaces and controls that ensure physical, logical, functional, and security compatibility between interfacing hardware, software, and facilities
Systems Engineering Information Management Plan	Outlines how SE-related information will be developed, acquired, managed, distributed, and stored throughout the project lifecycle
Risk Management Plan	Describes the approach, methods, procedures, and criteria for risk management and its integration into the program decision process
Configuration Management Plan	Documents the formal CM process to ensure that the integrity and continuity of the design, engineering, risk, and cost tradeoff decisions are recorded, communicated, and controlled
Verification Plan	Describes the overall verification program and enables full visibility of all verification activities. It includes test and evaluation planning. This is a crucial part of ensuring that the solution is being built right and evolving solutions comply with functional, performance, and design requirements.
Validation Plan	Lays out the methods by which the various work products, product components, and products will be validated. This may include a schedule, the applicable validation criteria, and any other item needed to ensure that the right product is being built to address the mission and enterprise needs.

In addition to the technical plans contained in the SEMP, there is additional planning that occurs during the life cycle and is often contained in standalone planning documents. The most notable standalone plans are:

- Life Cycle Plan
- Implementation Strategy and Planning Document (ISPD)

4.1.3.3 Life Cycle Plan (LCP)

Although life cycle planning may be included in the SEMP, it is usually a separate plan. In either case, the plan (or planning section) describes the tasks to perform life cycle activities. It provides the content and depth of detail necessary for full visibility of all lifecycle activities. The plan fully defines and describes each major activity and provides a general schedule and sequence of events. The plan includes the following planning sections: Integrated Logistics Support, Deployment and Transition, Real Property Management, Sustainment and Technology Evolution, and Disposal. Refer to Section 5.2: Life Cycle Engineering for additional information on these terms..

4.1.3.3.1 Integrated Logistics Support

This planning section will include maintenance; the maintenance support facility; direct-work maintenance staffing; supply support; support equipment; training, training support, and personnel skills; technical data; packaging, handling, storage, and transportation; and computer resources support..

4.1.3.3.2 Deployment and Transition

This section includes all tasks to prepare for and assess the readiness of a solution to be implemented into the NAS. Deployment planning tools, such as a tailored In-Service Review Checklist, shall be used to assist in identifying, documenting, and resolving deployment and implementation issues. Methods and techniques include, but are not limited to, a tailored application of generic tools; integration of checklist risks with other emerging risks (such as problem test reports from program tests and evaluation); development of action plans for resolution of checklist and other items; and documentation of the results of issue resolution and mitigation. Consistent deployment planning shall be visible in the contractor's Statement of Work and associated efforts.

4.1.3.3.3 Real Property Management

This section includes resources to determine whether real property is required, its acquisition costs, and the acquisition strategy (i.e.,buy or lease). If real property is being acquired, it must be included as real property in the Real Estate Management System and in any activities in the real property inventory process.

4.1.3.3.4 Sustainment and Technology Evolution

This section includes both sustainment and technology evolution activities as follows:

Sustainment

- Tracking and evaluating Reliability, Maintainability and Availability (RMA) performance and supportability issues
- Analyzing supportability issues caused by market-driven products
- Evaluating system or subsystem obsolescence

Technology Evolution

- Evaluating system or subsystem obsolescence, if evolving technology is appropriate
- Determining the most cost-effective means of avoiding projected supportability shortfalls Assessing integration of obsolescence-driven system changes with new requirements
- Evaluating the impact of engineering changes, performance shortfalls, or technological opportunities on integrated logistics support products and support services
- Periodically evaluating new technologies that may significantly reduce operations costs

4.1.3.3.5 Disposal

This section includes all activities associated with disposal management; dismantling, demolition, and removal; restoration; degaussing or destruction of storage media; and salvaging of decommissioned equipment, systems, or sites. The systems, assemblies, and other components that will be removed, disposed of, or cannibalized must be identified—as well as the agent responsible for disposal. An

assessment of the system to determine the need to salvage usable parts/subsystems from facilities to be decommissioned must be included in the planning. This is particularly important for items that are no longer being manufactured. An evaluation of environmental issues (including any hazardous materials), determination of disposition location, and removal of the system from the operational inventory must also be factored into the planning.

4.1.3.4 Implementation Strategy and Planning Document

The ISPD is the primary document within the AMS for planning the actions and activities to execute the project within the cost, schedule, benefits, and performance baselines. It is the recognized plan used to manage a project and contains the program Integrated Master Schedule, which includes milestones, accomplishments, and progress criteria. The ISPD relates tasks to program events and demonstrates logical, event-driven sequence of effort. It is directly traceable to the WBS, found in the SEMP, and facilitates resource planning; measures progress against planned efforts, ensures problem identification, and provides time-phased tasks and a framework to develop recovery and workaround plans.

Although the ISPD reflects selected SEMP planning elements, complete SE planning content is captured in the SEMP (or subordinate planning documents). Additional SE planning beyond that mandated in the ISPD ensures a more accurate costing of the program and a higher likelihood of success. Performance of these planned elements may reduce the percentage of requirements found in Operational Test. An ISPD is the responsibility of program management, who may delegate the writing and coordinating to SE. The ISPD is developed using the same basic planning steps used in developing the SEMP. The planning content for these SE elements will be a summarized extract from the SEMP to ensure consistency.

4.1.3.4.1 Inputs to the ISPD

The following inputs are necessary to develop the ISPD:

- Program objectives which detail the operational environments in which the system is expected to operate
- Program-specific guidelines
- Top-level program constraints and assumptions
- Program-specific schedule constraints and events
- Concept approach, including top-level conceptual alternatives, functional analyses, design support alternatives, and initial system evaluations
- WBS
- Any specified government or external standards to be employed in the program
- Other supporting technical plans to be presented at the Final Investment Decision

The ISPD is the responsibility of program management, who may delegate the writing and coordinating to SE. The ISPD is developed using the same basic planning steps used in developing the SEMP (see Section 4.1.3.1.3). Perform tailoring on planning documents only by deleting planning requirements; a rationale shall be provided for each deletion. The only allowable additions are those unique to the program.

4.1.3.4.2 Integrated Technical Management Inputs to the ISPD

SE planning directly relates to implementation of the relevant elements of the SE process defined in this SEM and is included as sections of the ISPD. It describes how the SE process is applied to the given program or project at a summary level with detailed SE implementation activities discussed in supporting technical plans (e.g., SEMP, Verification Plan, etc.). These planning sections become the tailored process that is implemented on a given program. All SE planning not included in other sections of the ISPD will be included at a summary level in the SE management planning section of the ISPD, with the details in the SEMP. All ISPD sections apply to every program; however, stakeholder direction or the nature of the program may dictate elimination of a planning section. For example, a program that deploys into a current facility rarely requires a real property section. The rationale for eliminating any ISPD sections or tailoring

any process must be documented, and the program manager must approve these actions. It is recommended that, as part of the ISPD, these planning sections be reviewed and changed whenever dictated by a change in the program or discovery of a discrepancy in the ISPD. Changes to any planning sections shall be coordinated with the SEMP and other associated plans. All plans shall be reviewed before each JRC milestone. After any plan is created following the SEM, it is recommended that the plan be provided as reference material for future plan developers. It is also recommended that, along with the plan to be achieved, comments are provided to continue improvement of the plan development process.

4.1.4 Technical Monitoring and Control

Technical monitoring and control is used to generate information or data needed to make technical decisions. It is a risk-reduction approach that works to ensure a project performs according to project plans, schedule, and budget while meeting the technical objectives and expectations of the stakeholder. Technical monitoring and control manages the progress of the technical aspects of a project. It measures or assesses progress against a plan, identifies variances, and provides sufficient information for informed decision making on corrective actions to take.

Technical monitoring is accomplished using techniques. An example of a **technique** is the measurement of certain technical characteristics of the system compared against a predetermined baseline or set of standards. Management tools and techniques are available to manage the program, mainly in the area of cost (resources) and schedule (time). While measures may differ in their focus (technical vs. nontechnical), they share a common basis of reference: the WBS.

The control aspect of the process is accomplished through the use of mechanisms. A **mechanism** is a control gate that assesses the progress of the system against criteria established for a given point in the system's lifecycle. Early in the system's lifecycle, these gates (or milestones) determine the degree and rate of system maturation. Later in the lifecycle, they focus on the adequacy of the system from a user's perspective. These gates typically take the form of technical reviews and audits, and should have predefined entry and success criteria. Reviews and audits occur at strategic points in the development cycle, and they are usually conducted in conjunction with, or in preparation for, a lifecycle phase milestone at which the decision to advance to the next phase is made. Figure 36 depicts the Product Development process in relation to the AMS phases. It also shows when the various reviews occur during the lifecycle. Section 4.1.4.7 provides an explanation of each review.

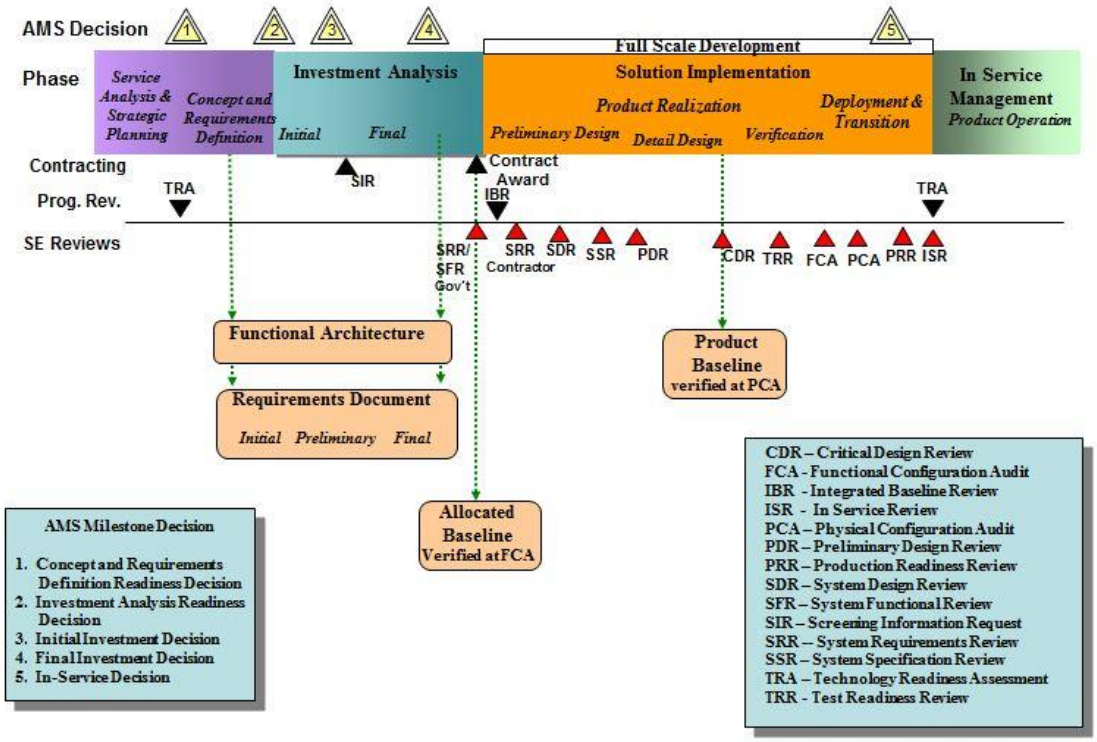


Figure 36: FAA Product Development Process

4.1.4.1 Technical Measurement

Technical Performance Measurement (TPM) is a key technique used in monitoring and assessing technical progress through a development program. TPM is a process to continuously assess and evaluate the adequacy of architecture and design as they evolve to satisfy program requirements and objectives. In other words, TPM is a quantitative way to pinpoint emerging design deficiencies, monitor progress relative to satisfying requirements, and developing trend information to assess program risks. Critical technical criteria or parameters are tracked as the analysis, design, and development activities progress from inception through system Initial Operational Capability (IOC). The assessment and evaluation is used to identify deficiencies that jeopardize the system's ability to meet pre-established performance requirements. Technical Performance Management produces periodic (typically monthly) trend and variance reports for all levels of management. For identified deficiencies, analysis is performed to determine the root cause and assess the impact on higher level parameters, interface requirements, and system cost-effectiveness. Alternate recovery plans are developed with cost, schedule, and performance impacts fully explored. Risk assessments and analyses are updated to reflect changes in the TPM profiles and current estimates, and impacts on related parameters. The SEMP establishes how technical assessments are accomplished and what measures will be used.

Critical Performance Requirements (CPR) are used in TPM. They are critical technical performance requirements that support critical operational needs and essentially measure the extent of success or failure of a design to meet those needs. It must be possible to project the evolution (or maturation) of CPRs over time toward the desired value at completion of development. The projection can be based on verification, validation, planning, or historical data.

For project metrics, the analog to TPM is Program Performance Measurement (PPM). PPM is used to track the current status of meeting selected program performance requirements. The most common application of PPM is the use of Earned Value Management (EVM). This is a management technique for integrating cost, schedule, technical performance measurement, and risk management. An EVM system

is established to objectively define the program baseline cost objectives and track them against performance and schedule.

For Earned Value to be effective, planning, budgeting and scheduling the authorized work scope (defined in the WBS) must be accomplished in a time-phased plan. As work is accomplished, it is "earned". The earned value is compared with the planned value for that same effort, providing a comparison of work accomplished against the plan. Any deviations to the plan are noted as cost or schedule variance. Actual costs are compared to the Earned Value to indicate an over or under run condition. Earned Value methodology provides an objective measure of performance, enabling trend analysis and evaluation of cost estimates at completion for multiple levels and stages of a project.

4.1.4.2 Technical Controls

In FAA, mechanisms are used to control the project progress. As stated earlier, mechanisms are control gates that assess the progress of the system against criteria established for a given point in the system's lifecycle. By setting entrance and exit criteria for each phase of work, the control gates are used to review and accept the work products completed for the current phase of work and also evaluate the readiness for moving to the next project phase. The Systems Engineering control gates in Figure 36 above are typically in the form of technical reviews or audits.

4.1.4.3 Technical Reviews

Technical Reviews assess the maturity of a project. Technical reviews, which are scheduled at strategic points within the development cycle, employ specific criteria tailored to the development effort. A well-structured technical review includes defined entry criteria, a basic set of common steps for every review, a predefined set of outcomes expressed in terms of exit criteria, and a set of metrics to measure success. These criteria verify the extent of technical progress made toward solving the identified capabilities shortfall.

A good technical assessment strategy addresses all of the prerequisites for conducting a technical review. Each review will have its own scope and objective; however, the inputs and outputs will generally remain the same from review to review and will simply mature from their status at the previous review. Once CPRs have been established for a program, the status of these CPRs will be included as inputs to enable measurement and tracking of the maturity of the design and risks to meeting the requirements. Table 17 lists typical inputs and outputs, referred to as entrance and exit criteria respectively, for a technical review.

Table 17: Technical Review Entry and Exit Criteria

Entry Criteria (Inputs)	Exit Criteria (Outputs)
Previously completed documents and products	Approved design documents
Shortfall Analysis Report	Gap analysis
SEMP	Updated SEMP
Requirements documents and specifications	Refined requirements documents and specifications
Architectures	Updated architectures or recommended changes
CPRs	Verification plans
Constraints	Updated Plans
Risk Mitigation Plans	Updated Risk Mitigation Plans

Entry Criteria (Inputs)	Exit Criteria (Outputs)
Test Plans	Test reports
Design Analysis Report (DAR)	Risk Management Reports
Functional analyses	Review Minutes
Test, evaluation, verification, and validation reports	Action item and issue documentation

4.1.4.4 Technical Review Process

A prerequisite for conducting a review is the approval of the technical planning documentation that defines the objective and scope of the review, entry criteria and items to be reviewed, review schedule, general approach for accomplishing the review, and review participants. The objectives of the review are defined in terms of success criteria or outcomes. Once the objectives and scope are established, the data to support these objectives can be identified. While the schedule in the technical planning documentation provides guidance for setting the review date, the specific date for the review is set once the entry criteria are determined to be in place. The approach can range from an informal review for small programs to incremental reviews for large complex programs replete with a standalone plan for the review. The generic steps for conducting a review are:

- Define review objectives and scope
- Establish success criteria, entry criteria, and approach to be used
- Set the date for the review and activities leading up to the review
- Create an agenda for the review
- Identify the items to be reviewed and the extent of review of each
- Compile and distribute review data package
- Assess readiness to proceed
- Collect comments to the data package
- Update data package
- Incorporate accepted changes
- Provide summary of concerns
- Update Risk Mitigation Plans
- Conduct review
- Document the review and publish minutes
- Compile action item and issues lists
- Track and close action items and issues

Technical Review Outputs

Outputs are the outcome of a successful technical review. They are a set of records that may be used to support a critical decision point or to verify that another key phase in the development has been reached. They consist of approved documents or approved changes to documents under review and may result in adding documents to the baseline. Typical review outputs include:

- Approved design documents
- Shortfall and gap analyses

- Requirements document(s) and specifications, including Interface Requirements Document (IRD) / Interface Control Document (ICD)
- Updated architectures
- Technical manuals
- Updated plans
- Risk Mitigation Plans
- Verification plan
- Validation plan
- Updated SEMP
- Approved reports
- Risk Management Reports
- Review minutes
- Action item and issue documentation

4.1.4.5 Tools and Metrics

Tools and metrics aid in the conduct of and success of technical reviews. Integrated Technical Management requires plan templates, word processing, display, and scheduling tools. Specific projects may tailor the template(s) to provide information pertaining to specific deliverables, tasks, and tools. Tools used to support technical reviews record the changes to and status of the technical baseline as the development proceeds. They include the requirements database, the technical performance measurement database, the risk database, and the project database used to document and monitor action items and issues.

Metrics are pre-established criteria that measure the success of a technical review. A successful technical review allows the project to proceed to the next phase. An individual technical review, due to its particular characteristics, may have additional specific metrics. They usually include:

- **The number of new requirements** (system or subsystem) that surfaces at later reviews compared to original requirements.
- **Number of Requests for Action (RFA)** resolved by formal action
- **Errata –** measured as the number of pages changed as a percentage of the total page count of the presentations.

4.1.4.6 Audits

Audits are used to verify that the developed system is consistent with the requirements baseline. Audits are conducted in two phases. The Functional Configuration Audit (FCA) uses testing to verify that the system functions and performs according to the specifications. The testing is at the configuration item level. The Physical Configuration Audit (PCA) verifies completion of any corrective actions identified through the FCA, as well as verifies that all baseline documentation is complete and accurately represents the as-built system.

In each case, an audit plan should be prepared to accomplish the following:

- Detail the audit processes to be used
- Identify the participants and their responsibilities
- Identify the item(s) to be audited
- Document the audit schedule

- Identify the documentation and supporting reference material to be audited
- Identify any supporting activities
- Furnish examples of PCA-related documentation, as appropriate

4.1.4.7 Systems Engineering Milestones

The FAA has established a set of reviews and audits to support its product development process. These are depicted in Figure 36. The generic use and structure of technical reviews and audits must be tailored for each review. The tailoring details are found in Appendix C, FAA System Engineering Milestones and Technical Reviews, along with some best practices and techniques for the following reviews.

Technology Readiness Assessment (TRA) – A multi-disciplined technical review that assesses the maturity of Critical Technology Elements (CTE) being considered to address user needs; it also analyzes operational capabilities and environmental constraints within the Enterprise Architecture framework. If a specific technology or its application is either new or novel, then the technology is considered a CTE. The TRA may score each CTE using nine Levels of Maturity (LOM), as shown in Figure 37.

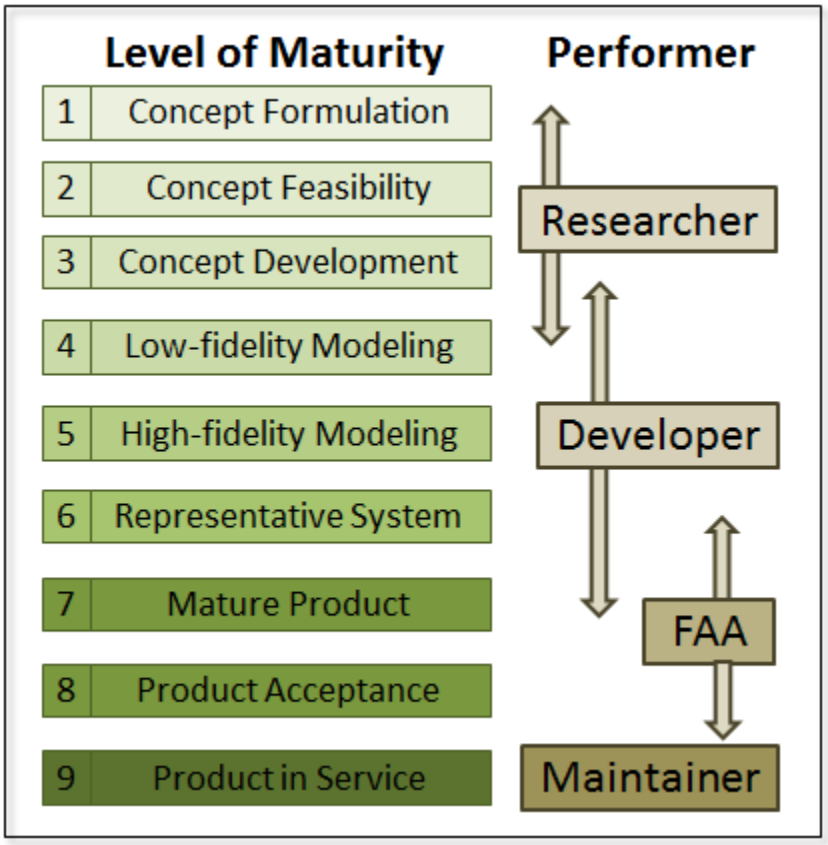


Figure 37: Technology Levels of Maturity

System Requirements Review (SRR) – At the program level, this is a formal internal FAA review to ensure that the system requirements have been completely and properly identified. It validates program cost, schedule, and performance in supporting milestone approvals. The SRR establishes the allocated baseline as the governing technical description, which is required before proceeding to the next AMS phase. At the contract level, the SRR is a formal, system-level review to ensure that system requirements have been completely and properly identified.

System Design Review (SDR) – This review evaluates the optimization, traceability, correlation, completeness, and risk of the system-level design to fulfill system functional baseline requirements. SDRs occur when the design definition effort has proceeded to the point where system characteristics are defined and configuration items are identified. Configuration Items are explained in Section 4.4: Configuration Management. The service team determines when this review is complete.

System Specification Review (SSR) – This formal review examines configuration item requirements as specified in the hardware and software specification. Its purpose is to establish the allocated baseline for preliminary design by demonstrating the adequacy of hardware and software requirements specifications. The SSR is complete when the services team determines that action items resulting from the review are sufficiently completed.

Preliminary Design Review (PDR) – This formal review confirms the preliminary design logically follows the contract level SRR findings and meets the requirements. It normally results in approval to begin detailed design and is often seen by many external organizations as the last viable point for effective technology insertion before the start of detail design.

Critical Design Review (CDR) – This formal review evaluates the completeness of the design, its interfaces, and suitability to start initial manufacturing.

Test Readiness Review (TRR) – A multi-disciplined review which ensures that the subsystem or system under review is ready to proceed to a system-level development test. The TRR determines the completeness of test procedures and their compliance with test plans and descriptions.

In-Service Review (ISR) – This formal review ensures that all activities necessary for the in-service decision are completed. This includes resolution of all support issues identified by the operating service organization and integrated logistics management team; completion of management actions arising from the in-service review checklist and independent operational assessment report (designated programs only); resolution of stakeholder issues; development of the in-service decision briefing and action plan; and concurrence of key stakeholders.

Functional Configuration Audit (FCA) – This formal review verifies that the system and all subsystems can perform all required design functions in accordance with their functional and allocated configuration baselines.

Physical Configuration Audit (PCA) – This formal audit establishes the product baseline as reflected in an early production configuration item.

Production Readiness Review (PRR) – This review determine if production engineering problems have been resolved, adequate planning accomplished and the design is ready for production. A PPR evaluates the complete production-configured system to determine if it correctly and completely implements all system requirements and that those requirements are traceable to the final production system.

4.1.5 Outputs

Integrated Technical Management is integral to all of the SE processes. The maintenance and evolution of all technical plans is best performed by the SE owner, by maintaining and reviewing the plans throughout the project life cycle. The following are the outputs of Integrated Technical Management:

- SEMP
- Supporting Systems Engineering Plans - Master Verification Plan (MVP), Lifecycle Plan (LCP), Configuration Management (CM) Plan, and any other applicable SE plans.
- SE updates to ISPD
- Updates to NAS Enterprise Architecture (EA)
- Technical Constraints
- Concerns, risks, and issues
- Approved SE or Design Documents

4.1.6 Process Improvement

A key part of planning is ensuring continuous process improvement. Process improvement begins by planning all programs / projects using approved tailorings (often insertion of a recommended organizational improvement to a standard process for use by the program) of standard organizational program / project processes. Business Process Definition or Re-engineering (BPR) establishes and maintains the organizational standard processes (often called “best practices”). Each program/project must have a mechanism to capture and report issues and improvements to process owners for use in analyzing, prioritizing, developing, and implementing improvements in the standard process in accordance with good CM practices. Even if the program/project cannot benefit from implementing solutions to issues or improvements that it identifies and reports, it contributes to organizational success by future programs / projects performing better, faster, or cheaper.

FAA can use International Organization for Standardization (ISO) 9001 and the ISO/IEC 33001-99 series of standards or FAA CMMI to implement improvements to the project processes during the project lifecycle. ISO provides a set of business process activities to ensure stakeholder satisfaction is achieved. CMMI describes characteristics for assessing efficient internal FAA processes and can be used by any organization pursuing process improvements.

The Enterprise “Software Process Improvement Capability Determination” (SPICE) process assessment model is an ISO conformant model that supports the assessment, improvement and implementation of processes. It brings an integrated approach for assessment and improvement, thereby alleviating the need to otherwise use multiple assessment models. Additional disciplines and sources were integrated into Enterprise SPICE. It may be used by any group looking to improve business performance in an integrated way. More information may be found at the website.

CMMI provides enterprise-wide best practice guidance and continues to evolve. It addresses management at several levels, acquisition, supply, engineering, the full product or service lifecycle, quality management, high performance, and a broad range of supporting processes.

Additional Information

For sources of information used to generate content throughout this section, see References.

To learn more about the topics in this section, see Additional Tools and Reading Recommendations.

4.2 Interface Management

Interface Management helps to ensure that all the pieces of the system work together to achieve the system's goals and continue to operate together as changes are made during the system's lifecycle. FAA systems interoperate with a variety of other systems, platforms, humans, and system elements. These connections and relationships are known as interfaces. An interface is the performance, functional, and physical attributes required to exist at a common boundary. It may be external, internal, functional, or physical. Interfaces must be precisely identified, controlled, and managed as early as possible and regularly throughout the system's lifecycle.

Interface Management identifies, describes, and defines Interface Requirements to ensure compatibility between interrelated systems and between system elements. It also provides authoritative means of controlling the interface design. The major outputs of Interface Management process are the Interface Requirements Document (IRD) and the Interface Control Document (ICD). The FAA uses the IRD to control interface requirements, while the ICD controls interface design. For more information about documenting interfaces, see FAA-STD-025f, Preparation of Interface Documentation. Note also that interface documents such as IRDs and ICDs must be configuration controlled, as described in Section 4.4: Configuration Management.

4.2.1 Interface Management Planning

Preparing for Interface Management requires developing an Interface Management Plan, often contained in the SEMP, for the project of interest. The Interface Management Plan includes the Interface Control Planning section that contains interface requirements and templates for preparing, revising, and processing ICDs unique to the project. The Interface Control Planning section also addresses supplier participation in the interface process.

At a minimum, a good Interface Management Plan should do the following:

- Provide the means for identifying, defining, documenting, and controlling the interfaces at all system levels
- Provide the means for changing the interfaces as required by the evolution of the design and for resolving interface incompatibilities
- Guide management, control, and documentation of all system functional and physical interfaces
- Establish the Interface Working Group (IWG) and its policies and procedures
- Appoint IWG chairperson, who also functions as planning coordinator and is responsible for developing and establishing the policies and process for identifying, defining, documenting, auditing, and controlling interfaces
- Provide requirements and templates for preparing, revising, and processing the interface documentation; identifies products
- Establish the participants of the interface management process and their responsibilities
- Establish the interface management schedule.

4.2.2 Inputs

The primary inputs to the Interface Management process are:

- ConOps
- Enterprise Architecture
- Any relevant Requirements Documents (NAS RD, pPR, fPR)
- ICDs for interfaces to current systems when replacing instantiated system(s)
- Trade study reports

- Physical and Functional Architecture
- SEMP, which contains the Interface Management Plan

4.2.3 Interface Management Process Steps

Interface Management includes the identification, definition, and control of all interfaces. It helps ensure that all of the system elements work together to meet project goals and objectives. It includes identification, definition, and control of interfaces. The Interface Management Plan helps facilitate interface activities.

Interface Management activities are as follows:

- Define the system boundary and interfacing systems
- Identify interfaces
- Develop Interface Requirements Documents (IRD)
- Create the Interface Control Document (ICD)
- Update interface documentation

4.2.3.1 Define the System Boundary and Interfacing Systems

A system boundary is the common interface between systems. At the beginning of a system's lifecycle the boundary is defined. Once the system boundary has been established, systems that currently are or will be co-functioning with the system being created or modified are defined. These systems can be internal or external to the new/modified systems.

- **Internal interfaces** are those interfaces within the defined system boundary.
- **External interfaces** are those interfaces outside the defined system boundary.

Definition of the system boundary and interfacing systems helps identify and define which systems elements are under design control of the new/modified system. These steps also show the expected interactions among system elements under design control and external and/or high-level and interacting systems outside the system boundary.

4.2.3.2 Identify Interfaces

After defining the system boundary and interfacing systems, identify the inputs and outputs flowing to and from the system across the interface boundary. These inputs and outputs establish the interchange across the interfaces. Interfaces are functional or physical.

- **Functional interfaces** clarify the functional responsibilities of the interfacing systems. Each interface has at least two associated functions, and because all performance requirements are traceable to functions, there shall be at least two associated interface requirements. Interface requirements shall be expressed in verifiable terms.
- **Physical interfaces** describe the relationship between the tangible system elements. They are used to define and control the features, characteristics, dimensions, and tolerances of one design that affects another. Physical interfaces include material properties of the equipment that affect the functioning of mating equipment. They also include the system's operating system.

An N^2 diagram is a visual matrix representing functional or physical interfaces between system elements. It is used as a systematic approach to identify, define, tabulate, design, and analyze functional and physical interfaces. (See Section 3.2: Functional Analysis for examples. Also see the Department of Defense Architecture Framework (DoDAF) Model.)

The N^2 diagram requires the user to generate complete definitions of all system interfaces in a rigid bidirectional, fixed framework. In this method, the functional or physical entities are placed on the diagonal axis; the remainder of squares in the matrix represents the interface inputs and outputs. The

functional interfaces identified in the functional N^2 diagram are documented in a Functional Interface list and the physical interfaces identified in the physical N^2 diagram are documented in a Physical Interface List.

4.2.3.3 Develop Interface Requirements Documents

The functional and physical interface lists are the primary input to the Interface Requirements Document (IRD). A set of interface requirements is generated from the list of physical and functional interfaces and is then documented in an IRD. The FAA IRD provides the interface requirements between two elements, including type of interface (*e.g.*, electrical, pneumatic, hydraulic, etc.) and the interface characteristics (performance, functional, or physical). It must be consistent with the final Program Requirements Document (fPRD). The IRD must be entered into Configuration Management.

Interface Requirements specify the performance, functional, or physical attributes that are required to exist at a common boundary. This boundary can exist between two or more functions, systems, system elements, configuration items, or systems. Interface Requirements shall be expressed in verifiable terms and follow the same formatting rules as system requirements. Refer to Section 3.3.2: Requirements Management for the characteristics of a good requirement.

4.2.3.4 Create the Interface Control Document

The IRD is used to create the Interface Control Document (ICD). The ICD identifies the design solution to satisfy the interface requirements in the IRD. It describes the detailed, “as-built” implementation of the interface requirements. The ICD is usually developed by the vendor and must be in compliance with the IRD. The IRD and ICD are the primary outputs of the Interface Management Process and both documents must undergo Configuration Management.

Data Interface Management for Service-Oriented Architecture and Web Services

FAA’s ongoing transition to the Next Generation Air Transportation System (NextGen) introduces a number of new advanced technologies and procedures. These bring into play new terminology and methodologies that require some readjustment in developing requirements and adaptation of specific inputs and outputs of the Interface Management process for data.

A key aspect of the transformation to the net-centric environment needed to achieve NextGen goals and objectives involves migration from systems that interact in a point-to-point fashion to systems that are based upon the concepts of Service-Oriented Architecture (SOA). SOA is an architectural paradigm that supports service orientation as a way of thinking in terms of services, service-based development, and the outcomes provided by services. The special case of services that leverage Web and Internet-based technologies, known as Web services, are commonly used in FAA as a means of realizing SOA. (For more information about SOA and Web services, see FAA-STD-070 section 1.3 “Basic Concepts.”)

Although adoption of SOA in FAA introduces many advantages (*e.g.*, platform and vendor diversity, use of open standards, reuse of existing assets, intrinsic extensibility, etc.), it also presents architects and developers with some challenges. When designing Web services, architects often have to provide highly specialized requirements for a loosely-coupled, standards-based, and platform-independent distributed system. Another task faced by developers of a SOA-based implementation is creation of a service description, which is the document that governs the mechanics of interaction between a service and its consumers by establishing the identity and functionality of the service, prescribing the service interface, and specifying the conditions for service invocation.

All these issues specific to service-based practices required adjustment of the existing interface management processes and resulted in two new documents explicitly tailored for Web service design and development: the Web Service Requirements Document (WSRD) and the Web Service Description Document (WSDD). These documents, which are designed to augment or replace ICDs in the area of service-oriented development, are governed respectively by Standard Practices: FAA-STD-070 Preparation of Web Service Requirements Documents and FAA-STD-065 Preparation of Web Service Description Documents. Note: IRD is required to define the requirements of Service Operations Center (SOC) via FAA-STD-025f, but ICD can be replaced with FAA-STD-070.

4.2.3.5 Update the Interface Management Plan, IRD, and ICD

As changes to requirements or design definition occur the IRD or ICD may need updated. Throughout Interface Management, the IRD shall satisfy the characteristics of a good requirement. The ICD must remain in compliance with the IRD, and the IRD must remain in compliance with the fPRD. Interface Management ensures all interface documents are updated to reflect any changes when design modifications occur or new requirements are added. The following steps comprise the change request process for the IRD and ICD:

- ***Step 1***: Prepare the interface change request (ICR) and provide the following information:
  - Description of the problem and the proposed change
  - Analysis showing how the change solves the problem
  - Analysis of how the change impacts system performance, effectiveness, and lifecycle costs
  - Analysis to ensure that the proposed solution does not introduce new problems
  - Descriptions of resources and estimate of costs associated with implementing the change
  - Statement of impact to system
- ***Step 2***: Provide change request to the Interface Working Group, which shall determine if the authorized Interface Change Request (ICR) is within the scope. In-scope ICRs shall be returned to the ICR originator and the custodian of the IRD/ICD for preparation and release of an interface requirement. Out-of-scope ICRs shall be forwarded to the program manager.
- ***Step 3***: Coordinate draft IRD/ICD with all affected organizations.
- ***Step 4***: Update IRD/ICD upon approval and include the approved ICR. Send updates to Configuration Management.

4.2.4 Outputs

The IRDs and ICDs are the primary outputs of the Interface Management Process. When documented and approved, the IRD is provided to all applicable organizations, while the ICD is provided to technical disciplines responsible for meeting its interface requirements, to customer and program management for coordination, and to the respective test and quality assurance organizations.

Additional Information

For sources of information used to generate content throughout this section, see References.

4.3 Risk Management

Risk Management is a standardized, continuous, and proactive process that identifies Risks, Issues, and Opportunities, assesses and analyzes Risk, Issues, and Opportunities, and effectively mitigates risks/issues, and leverages opportunities, to achieve program/portfolio objectives. Risk Management strives to limit the potential negative impact, also known as a Risk or Issue, before it occurs; while improving the chances of a positive outcome, also known as Opportunity, of occurring.

- Risk: A future event or situation with a realistic probability of occurring that may have a negative impact to the successful achievement of one or more program/portfolio objectives.
- Issue: An event or situation that has occurred or is certain to occur and has a negative impact to the successful achievement of one or more program/portfolio objectives.
- Opportunity: A future event or situation with a realistic probability of occurring that may have a positive impact to the successful achievement of one or more program/portfolio objectives.

A Risk, Issue, or Opportunity creates an impact exposure based on the combined effect of its likelihood and consequence, referred to as the "rating". Because the rating can appear and be treated at various levels and stages of a program, the Risk Management process must be applied at all levels of activity. The extent and depth of application of this process should be governed by the outcome(s) being supported.

This process is applied to ensure that a program or organization meets technical, schedule, and cost commitments; delivers a product or service that satisfies all stakeholders' lifecycle needs; and provides the expected benefit. Four lower-level objectives are established as part of the overall objective:

- Timely identification of Risk, Issues, and Opportunities - identifying a potential impact with sufficient lead time so that the team may implement appropriate alternate plans
- Consistent assessment of the rating - provides a structured decision making framework for prioritizing resource application
- Communication of Risk, Issues, and Opportunities actions across the program/organization - ensuring that all elements of the program or organization are aligned in addressing the Risk, Issue, and Opportunities
- Review of Risk, Issues, and Opportunities action performance.

4.3.1 Inputs

An expanded set of inputs capable of initiating Risk Management activities includes both program- and product-related data as shown in Table 18. Most of these inputs are developed and refined in the performance of other systems engineering processes. Each item may have an effect on the overall program. The second column indicates where details on each input may be found in the SEM or on the FAST website.

Table 18: Risk Inputs

Input	SEM Section
Risk Management Plan	4.1.3.2
System Engineering Management Plan (SEMP)	2.2.4.1
Integrated Safety Plan	5.6.3
Implementation Strategy and Planning	2.2.4.1
Test plans	4.1.4.3

Input	SEM Section
Integrated Program Schedule	4.3.1
Requirements	3.3
Mission Need and Concepts	3.3.1.2
Interfaces	4.2
Statement of Work	2.2.4.1
Issues/Concerns	
Decision Analysis Results	4.6
Design Analysis Results	7.2
Controlled Data and Reports	
Specialty Engineering Analysis Results	5.0
Safety and/or Security Assessments	5.6.3
Human Factors Assessments	5.4.3
Verification Results	4.7.2
Training Results	5.2.2
Maintenance Results	5.1.5
Operational Results	
Lessons Learned	5.6.2
Program Review Results	3.3.4.1
Analysis Criteria	4.1.1
External Environmental Forces	
ISAP (Internal Exhibit 300)	FAST
System Engineering Reviews	3.3.4.1
Contractor Outputs	
Technology	
Constraints	
Enterprise Architecture (EA)	2.2.3
Manufacturing/Production Information	2.2.5.1
Product Configuration Data	4.4.2
Resources/Budgets	2.2.2
FAA Policy	
AMS Documents	FAST
Corporate Strategy and Goals	
Contract	FAST

4.3.2 Risk Management Process Elements

The Risk Management process includes steps that result in identification of potential risks, analysis and assessment of risk, development of risk mitigation plans, implementation of the Risk Mitigation Plans, and monitoring of risk status. The process is iterative and is used throughout the program's lifecycle, with the nature of the risks changing to coincide with the lifecycle stage.

Roles and Responsibilities

Table 19 defines the responsibilities of the major participants in the risk management process.

Table 19: Risk Management Roles and Responsibilities

Role	Responsibilities
Organization Manager	• Establish and implement the organization's Risk Management Policy • Coordinate alignment of the organization's Risk Management Policy with the FAA Acquisition Management System (AMS) and the FAA Systems Engineering Manual (SEM) • Implement the organization's Risk Management Plan • Establish their respective Risk Management team [including the makeup of their Risk Management Board (RMB)] and allocate resources needed to support the organization's Risk Management Plan • Assist with managing Risks in their control in accordance to the organization's Risk Management Plan • Participate and chair their recurring Risk Management Board and Risk Review Meetings. Note: In the event that more than one manager is assigned to the same Risk Management Board, only one manager will chair the board. • Coordinate with their Risk Manager(s), and External Stakeholder senior leadership, when required
Risk Manager	• Support the Organization Manager in implementing the Risk Management Plan • Assist individual team members with all aspects of executing the organization's Risk Management Plan • Ensure Risk status and metrics are reported • Facilitate the organization's RMB and other supporting meetings • Assist with managing Risks in their control in accordance with the organization's Risk Management Plan • Assist with coordinating Risks in their control with external stakeholders • Represent Risk, Issue, and Opportunity Management for the program during internal and external Audits.
Risk Owner	• Support the organization's Risk Management Plan • Develop and manage their respective Risks in accordance with the Risk Management Plan • Assess their respective Risks, develop plans, and monitor results • Ensure their respective Risk status and metrics are reported to applicable program management • Participate in Risk Management Boards (RMB) and other supporting meetings
Risk Plan Owner	• Support the organization's Risk Management Plan • Assist the Risk Owner in creating plan options and help develop supporting steps • Manage their respective Risk plans in accordance with the Risk Management Plan • Assess their respective plans and monitor results • Participate in Risk Management Boards (RMB) and other supporting meetings
Risk Step Owner	• Support the organization's Risk Management Plan • Assist the Risk Owner in creating approach options and assist with the development of supporting steps • Manage their respective Risk steps in accordance with the Risk Management Plan • Assess their respective steps and monitor results • Participate in Risk Management Boards (RMB) and other supporting meetings
Organization Team Member/ External Stakeholder	• Identify new risks, issues, and opportunities • Assist in the analysis and assessment of Risks based on their individual areas of expertise and experience • Contribute to the identification of plan approach(es) for identified Risks and assist with the development of supporting steps. • Collaborate with the Risk Owner and program stakeholders to manage the Risk, within the scope of their areas of responsibility • Participate in Risk Management Boards (RMB) and other supporting meetings

Perform Risk Management

Risk management is a basic SE element of successful program management. When properly executed, risk management engages all disciplines and execution teams and is present in all program stages and phases. The steps in the process are:

1. Identify
2. Analyze & Assess
3. Develop Risk Plan
4. Execute Risk Plan, and
5. Track & Monitor

Based on results, program management may then determine:

- The schedule and budget reserve allocations
- How to measure overall program performance regarding each risk
- How much and what type of help is needed from other sources
- When to look at the process to see if the mitigation effort is working
- When to add mitigation efforts, costs, and milestones to the integrated program schedule and budget

This section describes the assignment of specific responsibilities for the management of risks, issues, and opportunities, and prescribes the documenting, monitoring, and reporting processes to be followed. This process is designed to provide the following:

- The framework for conducting Risk Management
- The identification approach, including data sources and techniques to be used
- The method for performing qualitative assessments, including likelihood and impact
- The methods for reducing the overall likelihood and impact, through the identification and implementation of tailored mitigation/enhancement plans
- The method for tracking and reporting to the oversight organizations

Risk Management Steps

Figure 38 depicts the five steps in Risk Management.

Figure 38: Risk Management Process Diagram

Step 1: Identify Risk

Risk, Issue, and Opportunity Identification is defined as a systematic effort to uncover events or situations that, if they occur, may hinder (risk/issue) or improve (opportunity) achievement of program/portfolio objectives. Risk, Issue, and Opportunities identification shall be performed during each stage of the program, or whenever significant changes occur in plans or program status.

Question to be asked are:

- Risks: What can go wrong?
- Issues: What has gone wrong?
- Opportunities: Where can something be improved?

Identification shall be performed during each stage of the program, or whenever significant changes occur in plans or program status. Circumstances requiring assessment include:

- Programmatic changes (including schedules and cost milestones)
- Unfavorable trends in Technical Performance Measures, predicted system performance, schedules, and financial status
- Design/program/peer reviews
- Change proposals (including proposed changes in requirements)
- Occurrence of a major unforeseen event
- Newly identified risks/issues/opportunities
- Special assessments at the direction of agency management

- Changes or risks in interdependent programs
- Environment changes

Participants in risk identification include all stakeholders, users, suppliers, and execution teams. Teams consider all likely risk sources in identifying potential risks to the program/project. Risk identification is based on the current program/project goals supported by the associated technical, schedule, and cost requirements and plans.

Each risk has a "risk realization date". This date is when the negative consequence of the outcome of the risk occurs. It is very important to identify and document this date as early as possible to ensure that only active risks consume the organization's attention and resources.

Potential Sources of Risk

Program risk originates from three basic areas – technical (or performance), schedule, and cost. The determination of which area or category a risk falls into is determined by its root cause.

- **Technical risk** is based on the likelihood that the program as planned will be unable to deliver a product or service to satisfy the technical requirements. As such, well-documented, defined, and quantified technical requirements are necessary to define a technical risk.
- **Schedule risk** results from the likelihood that the program actions may not be accomplished in the planned program timing. A detailed program schedule identifying each accomplishment and the critical path is necessary to develop schedule risks.
- **Cost risk** results from the likelihood that the program may not accomplish planned tasks within the planned budget. A detailed budget, in which the cost of each accomplishment is specified and any management reserve is known, is needed to determine a cost risk. Potential loss of funding is typically not a program risk because the funding decision is made at the Agency level, and the financial risk to the program occurs once a decision has been made to allocate the existing Agency funding among programs and/or organizations. Within the FAA risk process, cost is the expenditure required for a resource and the end product produced by that resource. Budget is the forecast of all costs planned for a given project, and funding is the supply of money provided to accomplish it.

A risk can affect a project's technical requirements baseline, its cost, its project schedule, or any combination of the three. Defining a risk based upon these sources aids in identifying additional aspects of the risk, assists with the management of the risk, and provides a framework for identifying potential patterns in related risks. If applicable, the process described in this section a user to identify a risk based upon multiple facets (primary and secondary).

Many sources must be considered for each risk area. For technical risk, likely sources include technology maturity, complexity, dependency, stakeholder uncertainty, requirements uncertainty, and testing/verification failure. Sources of schedule risks may include incomplete identification of tasks, time-based schedule (as opposed to event-based schedule), critical-path scheduling anomalies, competitive optimism, unrealistic requirements, and material availability shortfalls. Cost risks may stem from an uncertain number of production units, supplier optimism, added complexity, changes in economic conditions, competitive environment, supplier viability, and lack of applicable historical data.

A program's acquisition strategy generates risks in its own right. Development programs using proprietary or custom designs are different in nature from those using COTS solutions.

The knowledge domains of safety and security impose additional criteria or gates as part of their identification process. In the case of safety, the process commences with an analysis, which identifies potential hazards that are the basis for identifying safety-related risks. Safety does not identify a risk until a hazardous situation has been identified.

Information security engineering also utilizes a series of gates prior to identifying a risk. Security is concerned about the existence of viable threats, which may exploit a system's vulnerability to cause

harm. The combination of a viable threat coupled with vulnerability in the system that is capable of being exploited by the threat is necessary before the security community moves to declare a security risk.

Risk Identification Methods

Risk identification begins at the lowest feasible level and includes inputs from all stakeholders. Anyone may identify a potential Risk, Issue, and Opportunity. Teams consider all likely sources or root causes, not symptoms, in identifying potential Risk, Issue, and Opportunities. Risk identification is based on the current program/project acquisition strategy and goals supported by the associated technical, schedule, and cost requirements or any combination of the three. Defining a Risk, Issue, or Opportunity based upon these goals aids in identifying additional aspects, assists with the management of, and provides a framework for identifying potential patterns in Risk, Issue, and Opportunities. Potential sources of Risk, Issue, and Opportunities include but are not limited to the following:

- Technology maturity
- Dependency on other programs
- Requirements uncertainty, including safety and security
- Testing/verification failure
- Program timeline
- Changes in economic conditions
- Safety Hazards
- Security Threats or Vulnerabilities

It is recommended that experts review previous programs to determine that Risk, Issue, and Opportunities related to their domain(s) have been completely identified. It is also recommended that similar programs be reviewed for potential Risk, Issue, and Opportunities. This may be achieved using any combination of methods, such as group discussions, interviews, trend/failure analysis, Risk, Issue, and Opportunity Scorecards, lessons learned, trade studies, best practices, metrics, and acquisition documentation.

Risk, Issue, and Opportunity Statements

During the Risk Identification step, it is important to formulate a concise and accurate statement so that management and stakeholders clearly understand the Risk, Issues, and Opportunities. A properly worded statement improves the ability to properly analyze the risk, make accurate assessments, and select appropriate actions. Figure 39 depicts examples of well-written risk statements.

The purpose of a Risk, Issue, or Opportunity statement is to enable managers, program team members, and stakeholders to understand the source and nature of the Risk, Issue, or Opportunity. Understanding the Risk, Issue, or Opportunity statement will improve one's ability to analyze the Risk, Issue, or Opportunity properly, make a reasoned assessment of impact, and effectively communicate the Risk, Issue, and Opportunity information to those within and outside of the program.

Statement Constructs:

Risk: "If [specific cause], then [specific impact]."
Issue: "Due to [specific cause], [specific impact] was experienced."
Opportunity: "[Specific impact] may be achieved if [specific cause] can be accomplished."

	Statement Example

Risk	If ABC Technical Operations (Tech Ops) training requirements are not met prior to the September XX, 20XX Initial Operating Capability (IOC) date at XYZ TRACON, then the IOC at XYZ may be delayed.
Issue	The planned milestone date (9/XX/20XX) to complete the 100% Engineering Site Design for the second site was not met because precision 1A surveys were not accomplished in time due to stop work related to uncertainty in the safety analysis.
Opportunity	If the XX program is able to leverage YY organizations ZZ demonstration activities to positively influence the planned 2016 flight tests for XX program, then XX program will be able to accelerate development, improve the fidelity of the work to ensure industry buy-in and achieve up to $N million in cost savings.

Figure 39: Risk, Issue, and Opportunity Statement Examples

Step 2: Analyze and Assess

Risk, Issues, and Opportunity Analysis is defined as an evaluation of the identified Risk, Issues, and Opportunities to determine possible outcomes, the likelihood of those events occurring, and the impacts of the outcomes. Step 1: Identification, fully defines both the “specific cause” and the “specific impact” of the Risk, Issues, and Opportunities. This allows program management to sufficiently analyze and assess the Risk, Issues, and Opportunities. The likelihood of occurrence and the impact if it occurs are individually evaluated using the Risk, Issue, and Opportunity Scorecard definitions and are then combined into a single Risk, Issues, and Opportunity rating. Two different components make up the rating, Level (High, Medium, and Low) and Alpha (Likelihood)-numeric (Impact), which assists program managers with prioritizing (most severe to least severe) their resources and efforts. The impact facet (cost, schedule, and/or technical) is also tracked. All assumptions considered when analyzing the Risk, Issues, and Opportunities are documented. The rating (assessment) is reviewed and an approval determination is made. In addition, analysis of Risk, Issues, and Opportunities may include more in-depth qualitative and/or quantitative analysis techniques.

Risk, Issues, and Opportunities are continuously re-analyzed and re-assessed. Re-analysis includes evaluating all components of the Risk, Issues, and Opportunities for updates including but not limited to the statement, rating, and plan. This evaluation includes identifying Risk, Issues, and Opportunities for RMB reassignment, considering Risk, Issues, and Opportunity Status changes, as well as evaluating a Risk, Issues, or Opportunities need to be transferred to an external stakeholder.. Similar to when a Risk, Issues, and Opportunities is initially assessed, approval of all proposed changes during the re-assessment is required.

Risk Assessment

Note that in the context of risk management, the terms “consequences” and “impact” may be used interchangeably, as well as the terms “probability” and “likelihood”.

Risk Likelihood Determination

Risk likelihood is the probability that a negative event will occur. The definitions in Table 20 will be used as a guide in assessing likelihood

.

Table 20: Risk Likelihood

Level	Likelihood	Description	Probability
A	**Low** Not Likely	The chance of a negative outcome based on existing plans is not likely. This likelihood level assessment should be based on evidence or previous experience and not on subjective confidence. This assessment level requires the approach and process to be well understood and documented. Little or no management oversight will be required.	0% - 10%
B	**Minor** Low Likelihood	There is a low likelihood but reasonable probability that a negative outcome is possible. Present plans include adequate margins (technical, schedule, or cost) to handle typical problems. This assessment level requires the approach and processes to be well understood and documented. Limited management oversight will be required.	10% - 33%
C	**Moderate** Likely	A negative outcome is likely, or the current approach and processes are only partially documented. Alternative plans or methods exist to achieve an acceptable outcome even if the risk is realized. Present plans include adequate margins (technical, schedule, or cost) to implement the workarounds or alternatives to overcome typical problems. Significant management oversight will be required.	33% - 66%
D	**Significant** Highly Likely	A negative outcome is highly likely to occur, or the current approach and processes are not documented. While alternative plans or methods are believed to exist to achieve an acceptable outcome, there are not adequate margins (technical, schedule, or cost) to implement the workarounds without impacting the program management reserves in performance, schedule, or cost. Significant management involvement is required.	66% - 90%
E	**High** Near Certainty	A negative outcome is going to occur with near certainty. No alternative plans or methods have been documented. Alternatively, the risk item has yet to be evaluated adequately to be well understood, so there is a high level of uncertainty about the program success. Urgent management involvement is required.	90% - 100%

Risk Impact Determination(s)

Impact is a measure of the specific impact (cost, schedule, and/or technical) on program goals if the risk were to occur. The following definitions in Table 21 will be used as a guide for determining risk impact. Note that the affected program baseline is an input to the process for determining the impact level.
Note: Programs may augment the FAA scorecards with additional impact definitions to assist with the management of their risks. Programs should document all Risk, Issue, and Opportunity Management *practices in the Risk Management Plans including but not limited to the augmentation of the FAA Scorecard. – see Section 4.1: Integrated Technical Management for more details.*

Table 21: Risk Impact

Level	Impact	Technical	Schedule	Cost
1	**Low** Program success not impacted	Technical goals will still be met.	Schedule will still be met.	0% < Cost increases <= .1%
2	**Minor** Negligible impact to program success	Minor performance shortfall (within acceptable limits); no design or process change needed.	Schedule slip but able to meet key dates with additional activities or effort; critical path not affected.	.1% < Cost increases <= 1%
3	**Moderate** Limited impact to program success	Moderate performance shortfall; alternatives available, with minor design or process change needed.	Some key dates missed; alternatives available; critical path not affected.	1% < Cost increases <= 5%
4	**Significant** Program success could be jeopardized	Unacceptable performance; alternatives available, with significant design or process change needed.	Critical path affected; alternatives available; major milestones not affected.	5% < Cost increases <= 10%
5	**High** Program success in doubt.	Unacceptable performance; alternatives not available.	Cannot achieve major milestones; rebaseline required.	Cost increases > 10%

Risk Level Determination

The assessments performed above – likelihood and impact – determine whether the risk is classified as low, medium, or high, as seen in Figure 40. This rating allows management to effectively assign resources to those risks that are deemed more critical to the program.

Low Risk: Has little or no potential for increase in cost, disruption of schedule, or degradation of performance. Normal emphasis/effort, coordination, and normal monitoring will probably overcome difficulties.

Medium Risk: May potentially cause some increase in cost, disruption of schedule, or degradation of performance. Special emphasis, close coordination, and close monitoring will probably be able to overcome difficulties.

High Risk: Likely to cause significant increase in cost, disruption of schedule, or degradation of performance. Concerted and continual emphasis, coordination, and close monitoring will probably not be sufficient to overcome difficulties.

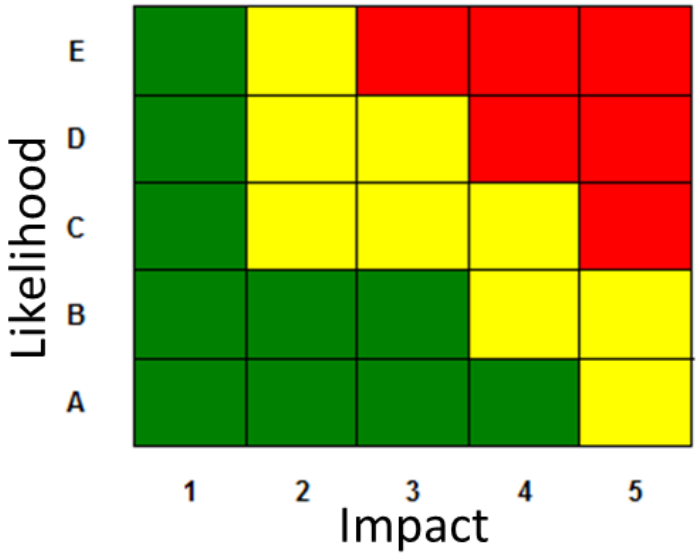


Figure 40: Risk Grid or Probability Impact Diagram

Issue Assessment

Issue Likelihood

Since an issue has occurred or is certain to occur, there is no need to assess the likelihood of occurrence.

Issue Impact

The Risk Impact definitions shown in

Table 21 are used as a guide for determining issue impact. Note that the affected program baseline is an input to the process for determining the impact level.

Issue Level

The impact assessment performed above defines whether the issue level is classified as low, medium, or high, as shown in Figure 41. This allows management to effectively assign resources to those issues that are deemed more significant to the overall success of the program**.**

Low-level Issue: Little or no impact for increase in cost, disruption of schedule, or degradation of performance. Normal emphasis/effort, coordination, and normal monitoring will overcome difficulties.

Medium-level Issue: Some increase in cost, disruption of schedule, or degradation of performance. Special emphasis, close coordination, and close monitoring will be able to overcome difficulties.

High-level Issue: Significant increase in cost, disruption of schedule, or degradation of performance. Concerted and continual emphasis, coordination, and close monitoring will not be sufficient to overcome difficulties.

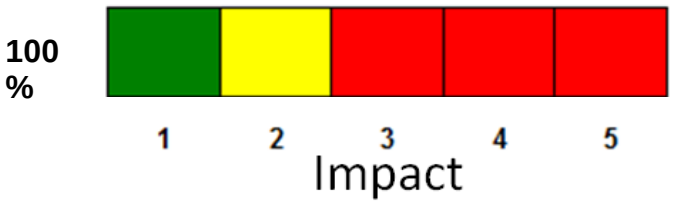


Figure 41: Issue Level Grid or Probability Impact Diagram

Opportunity Assessment

Opportunity Likelihood

Opportunity likelihood is the probability that a positive event will occur. The definitions in Table 22 will be used as a guide in assessing likelihood.

Table 22: Opportunity Likelihood

Level	Likelihood	Description	Probability
A	**Low** Not Likely	Unlikely to achieve the opportunity; no known processes or alternatives are available.	0% - 10%
B	**Minor** Low Likelihood	Existing approach and processes cannot achieve the opportunity, but different approach(es) might.	10% - 33%
C	**Moderate** Likely	Existing approach and processes may achieve the opportunity, but alternative approach(es) may be required.	33% - 66%
D	**Significant** Highly Likely	Existing approach and processes may achieve the opportunity based on similar cases.	66% - 90%

E	**High** Near Certainty	Expected to achieve the opportunity based on existing approach and processes.	90% - 100%

Table 6: Opportunity Likelihood

Opportunity Impact

Opportunity impact is the positive effect on program goals if the opportunity is achieved. The definitions shown in Table 23 will be used as a guide for determining impact. Note that the affected program baseline is an input to the process for determining the impact level.

Note: Programs may augment the FAA scorecards with additional impact definitions to assist with the management of their risks. Programs should document all Risk Management practices in the Risk Management Plans including but not limited to the augmentation of the FAA Scorecard. For more details, see Section 4.1 Integrated Technical Management.

Table 23: Opportunity Impact

Level	Impact	Technical	Schedule	Cost
1	**Low** Program not impacted	Slight increase to claimed benefits.	Slight acceleration of schedule, but key dates not impacted; critical path not affected.	0% < Cost savings <= .1%
2	**Minor** Negligible impact to program	Some increase to claimed benefits.	Some acceleration of tasks, but key dates not impacted; critical path not affected.	.1% < Cost savings <= 1%
3	**Moderate** Moderate impact to program	Moderate increase to claimed benefits.	Acceleration of some key dates; critical path moderately improved.	1% < Cost savings <= 5%
4	**Significant** Major impact to program	Major increase to claimed benefits.	Major acceleration of schedule; critical path optimized.	5% < Cost savings <= 10%
5	**High** Significant impact to program	Significant increase to claimed benefits.	Significant acceleration of milestones; rebaseline required.	Cost savings >10%

Opportunity Level

The assessment performed above (likelihood and impact) drives whether the opportunity is classified as low, medium, or high, as shown in Figure 42. This rating allows management to effectively assign resources to those opportunities that are deemed more significant to the overall success and enhancement of the program.

Low Opportunity: Minor increase in benefits to the program with minimal schedule acceleration and cost savings, or minor expansion of program benefits with significant schedule duration and costs incurred. Concerted and continual emphasis, coordination, and close monitoring will probably not be sufficient to achieve the opportunity.

Medium Opportunity: Some increase in benefits to the program with moderate schedule acceleration and cost savings, or some expansion of program benefits with moderate schedule duration and costs incurred. Special emphasis, close coordination, and close monitoring will probably be able to achieve the opportunity.

High Opportunity: Significant increase in benefits to the program with maximum schedule acceleration and cost savings, or significant expansion of program benefits with negligible schedule duration and costs incurred. Normal emphasis/effort, coordination, and normal monitoring will probably achieve the opportunity.

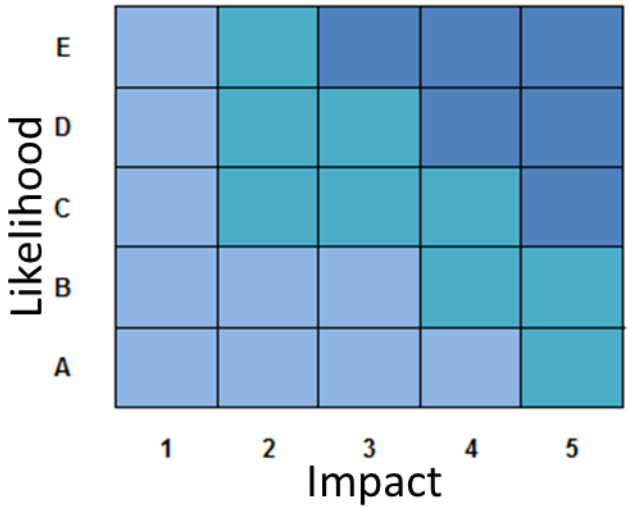


Figure 42: Opportunity Level Grid or Probability Impact Diagram

Escalate or Transfer Risk, Issues, and Opportunities

Risk, Issues, and Opportunities are continually evaluated to determine if they are being successfully managed. Risk, Issues, and Opportunity Management allows for two different types of escalation: for either visibility or management purposes. Risk, Issue, and Opportunities that cannot be managed at their respective board are escalated to an appropriate board. Both the originating organization and the destination organization must approve the movement and the destination organization agrees to actively work to achieve the desired results. Possible reasons for escalation to a higher tier level are:

a. Potential loss (R/I) or improvement (O) of service impacting the NAS

b. Could jeopardize (R/I) or improve (O) achievement of program goals and/or objectives
c. Cannot be mitigated (R/I) or achieved (O) at the lowest management level
d. Interdependent Risk, Issue, and Opportunities which could jeopardize (R/I) or improve (O) an external stakeholder's activity

There may be cases where management at different levels in the organization request or require situational awareness of Risk, Issues, and Opportunities that reside under their purview but do not require a change in Risk management responsibilities. This type of escalation is for visibility only.

Disposition of Risk, Issues, and Opportunities

The Risk, Issues, and Opportunities Owner proposes that the Risk, Issues, and Opportunities be dispositioned in accordance with the Risk, Issue, and Opportunity Status definitions of Table 8 (Section 2.7) when a Risk, Issue, or Opportunities meets one or all of the following criteria:

- If the Risk, Issues, and Opportunity action plan has been successfully implemented; the intended goals have been achieved.
- If the critical milestones have passed and the Risk, Issues, and Opportunities has not been realized.
- If the Risk or Issue no longer poses a threat to schedule, technical functionality, and/or costs,
- If the Opportunity is no longer applicable
- If the Risk, Issues, and Opportunity technical approach has changed.
- If a Risk, Issues, and Opportunity has not been successfully managed.

The Risk Management Board discusses the proposed disposition with the owner or designated representative present. Once approval is granted, the Risk, Issues, and Opportunity status is updated and the associated documentation is maintained for archival purposes.

Transfer of Risk, Issues, and Opportunities
During assessment and analysis, management might also determine that certain Risk, Issues, and Opportunities are no longer able to be properly managed within their Line of Business. Intra-agency coordination allows these Risk, Issue, and Opportunities to be transferred to other lines-of-business.

Step 3: Develop Risk Mitigation Plan

Risk plans consist of a Plan Strategy, Plan Description and discrete steps for each applicable Risk, Issues, and Opportunity, and must be developed for all Risk, Issues, and Opportunities with a Plan Strategy of Control and/or Research and Knowledge. Risk Plans should be evaluated in terms of feasibility, expected effectiveness, cost (including use of management reserve) and schedule implications, the effect on the system's technical performance, and the most suitable strategy selected. The objective of Risk Plans is to implement appropriate and cost-effective Risk, Issues, and Opportunity actions to address the Risk, Issues, and Opportunities. The goals of the plans are as follows:

- For risks, the objective of the plan is to reduce the likelihood of occurrence and/or negative impact if the risk is realized.
- For issues, the objective of the plan is to reduce the issue's negative impact
- For opportunities, the plan outlines the steps to improve the likelihood and/or positive impact.

A contingency plan description can be developed if there is concern about the success of the first-choice plan. When it is determined that the first-choice plan is not achieving the desired results, the Risk, Issue, and Opportunities will be reassessed & analyzed in accordance with the contingency plan description.

Risk, Issues, and Opportunity handling (planning, implementation, and tracking) is one of the core components of risk management. Risk mitigation plan implementation requires a conscious management decision to approve, fund, schedule, and implement one or more risk mitigation actions. Risk mitigation

plans and mitigation actions are reviewed frequently at major reviews, program reviews, acquisition reviews, and milestone reviews. Risk mitigation actions fall into one or more of the following strategies shown in Table 24.

Plan Strategy

The Risk management process provides the framework for developing plans to take action, or deliberate decisions to take no action, in order to address program Risk, Issue, and Opportunities. The plan strategy options are defined in Table 24. For all identified Risk, Issue, and Opportunities, the various strategies should be evaluated in terms of feasibility, expected effectiveness, cost and schedule implications, the effect on the system's technical performance, and the most suitable strategy selected.

Table 24: Plan Strategy Definitions

Plan Strategy	Definition
Avoid	Avert the potential of occurrence and/or impact by eliminating the risk/issue or protecting the program from its impact.
Transfer	Shift the Risk, Issue, or Opportunity to another program, giving the receiving program responsibility for its management..
Control	Develop options and alternatives for taking action to address the likelihood and/or impact of the Risk, Issue, or Opportunity. Note: This is the most common plan strategy.
Accept	Accept the likelihood/probability and the impacts associated with a Risk, Issue, or Opportunities occurrence. Program team decides to acknowledge the Risk, Issue, or Opportunities and not to take any action unless it occurs. This strategy is adopted where it is not possible or cost effective to address a specific Risk, Issue, or Opportunity in any other way.
Research and Knowledge	Address the Risk, Issue, or Opportunities through expanding research and experience. It may be possible to effectively manage Risk, Issue, and Opportunities simply by enlarging the knowledge pool, leading to reassessment that reduces the likelihood or provides insight into how to achieve the suitable impact.

Plan Approach

Once a strategy has been chosen, a high-level plan description is generated. This description can include the use of multiple methods (approaches) for addressing the Risk, Issues, and Opportunities. Individual plan steps are then defined to support the methods. Alternatives include detailed plans for mitigating the risk in several small, sequential steps; alternative steps; or entirely new (non-baselined) approaches to accomplishing the program. The mitigation steps are the major milestones of the mitigation plan.

Further, contingency plans are identifiable alternatives, which may be implemented if a mitigation plan fails, and the risky event or conditions occur with more serious consequences than anticipated. Contingency plans need not be detailed until they become the primary approach to reducing the risk.

For instance, the risks associated with selecting a COTS-based acquisition approach have known risk mitigation strategies. These strategies need to be included in a decision analysis when comparing investment or acquisition approaches. Because COTS has an inherent set of risks that are market driven, most of the risk mitigation strategies fall into the "Control" category in order to anticipate and

reduce the risks to acceptable levels. More information on COTS risks and mitigation strategies may be found in the FAA COTS Risk Mitigation Guide.

The risk level is the first criterion used to determine the need for a risk mitigation plan. As specified in the Risk Management Plan (RMP), risks that typically fall into the medium or high categories require risk mitigation plans. Risks that are assessed as low typically do not require mitigation plans but may have certain aspects that would be prudent to monitor. If this is the case, risk mitigation plans may be formally or informally implemented for these low risks based on the specific governing RMP.

It is essential that plan implementers have a thorough understanding of the root cause of the risk to be mitigated. This may be accomplished with a good summary statement of the risk (see Figure 39). Do not state the risk in terms of its mitigation plan. It is recommended that the status also include a summary of risk mitigation efforts that references more detailed documentation. A Risk Mitigation Plan Summary is used to report the analysis and actions on an individual risk.

The risk mitigation plan documents the specific steps to be implemented, the sequence in which they are to be implemented, and the points in time at which they are to be implemented. Developing a risk mitigation plan includes assessing the expected outcome following implementation. It is recommended that the same method initially used to assess the risk, such as risk templates, be used to provide a forecast of the risk level after completion of each action of the risk mitigation plan.

Plans consist of a series of steps that when completed reduce the rating of the Risk, Issue, or Opportunity to an acceptable threshold for the program. When developing the plan steps, interdependences and due dates should be identified and considered. This level of detail will enable the organization to monitor the progress of reducing the likelihood and impact of risks and issues and achieving desired opportunities. Also, it is possible to develop multiple plan approaches simultaneously in order to determine the best plan.

There are several times during a program's /project's life cycle that may provide an appropriate decision point that may trigger a re-assessment of a Risk, Issues, or Opportunity. Examples of appropriate placement of those decision points include, but are not limited to:

- Entry into a new phase
- Identification of new stakeholder(s)
- Key program milestones
- Significant steps in the action plan

The expected impact of each mitigation event on risk level may be projected using a waterfall, or "burn down" chart, an example of which is shown in Figure 43.

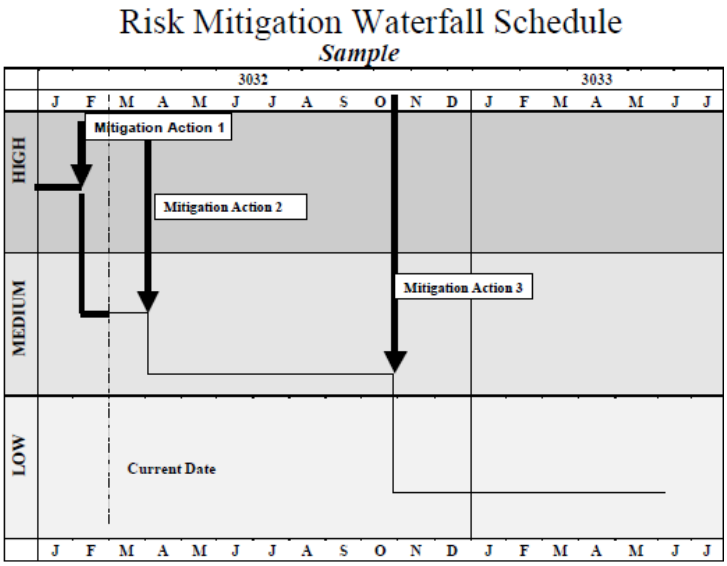
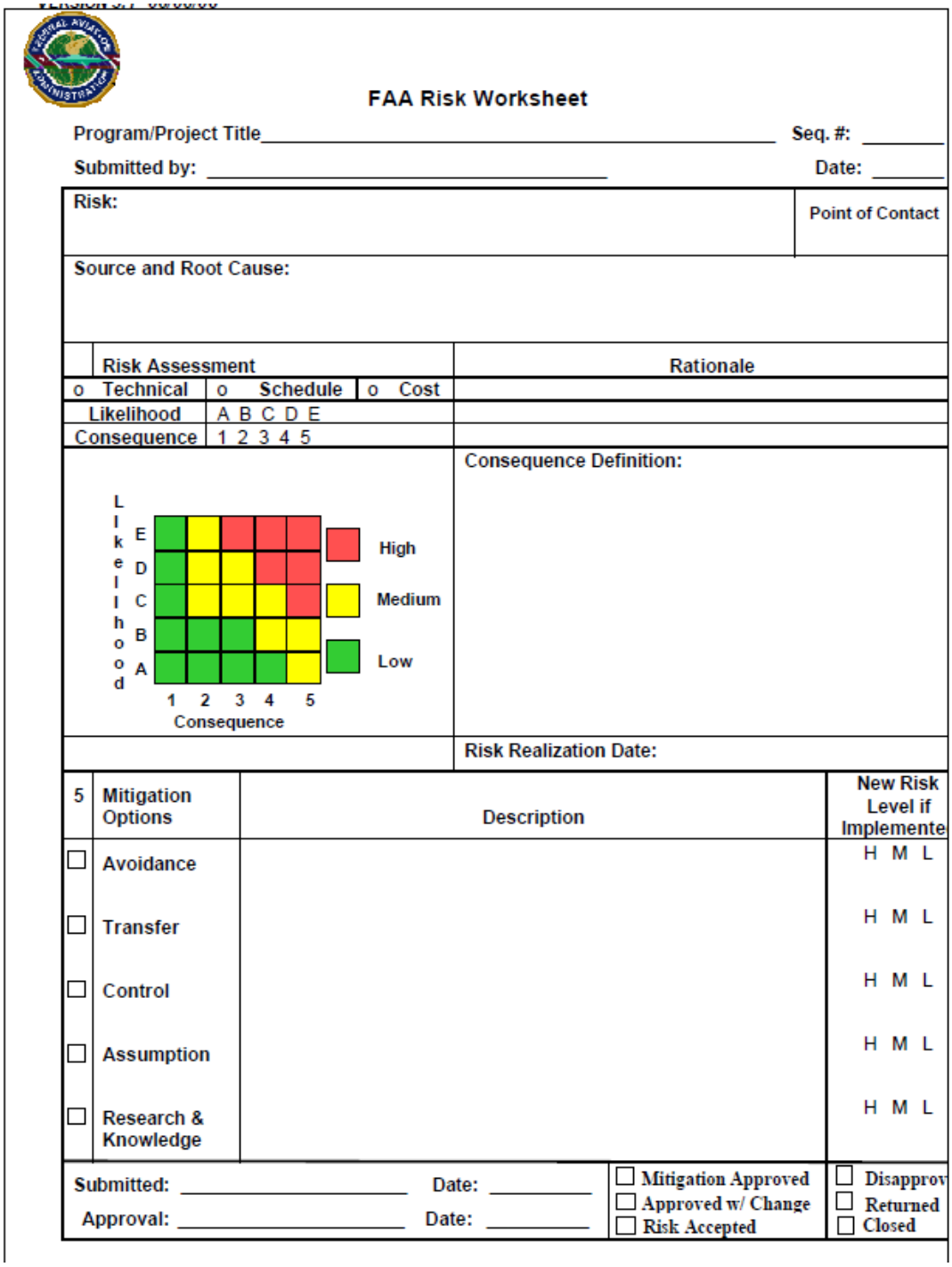


Figure 43: Risk Mitigation Waterfall Chart

A Risk Worksheet may be used by programs to guide the practitioner through the first three tasks in the Risk Management process: identify risk, analyze risk, and develop mitigation planning. When a risk mitigation plan has been prepared, management reviews and approves it based on criteria defined in the RMP. Figure 44 is an example of a Risk Worksheet.



FAA Risk Worksheet

Program/Project Title_____ Seq. #: _____

Submitted by: _____ Date: _____

Risk:	Point of Contact
Source and Root Cause:	

	Risk Assessment			Rationale
o Technical	o Schedule	o Cost		
Likelihood	A B C D E			
Consequence	1 2 3 4 5			

Consequence Definition:

Risk Realization Date:

5	Mitigation Options	Description	New Risk Level if Implemente
☐	Avoidance		H M L
☐	Transfer		H M L
☐	Control		H M L
☐	Assumption		H M L
☐	Research & Knowledge		H M L

Submitted: _____ Date: _____ ☐ Mitigation Approved ☐ Approved w/ Change ☐ Risk Accepted ☐ Disapprov ☐ Returned ☐ Closed

Approval: _____ Date: _____

Figure 44: Risk Worksheet Example

Step 4: Execute Risk Management Plan

Once the organization decides on a Risk Plan, it shall be implemented and carried out. Risk Plan execution may require that the associated specific tasks be incorporated into the planning, scheduling,

budgeting, and cost-accounting systems used by the program. Incorporating the Risk Plan steps directly into the program schedule keeps management and the program team aware of the need to manage the Risk, Issue, and Opportunities to achieve the desired results. Activities are shared with and communicated to all stakeholders.

Step 5: Track and Monitor

Existing Risk, Issues, and Opportunities are tracked and monitored periodically, on an event-driven basis, or continuously. This includes obtaining Risk, Issues, and Opportunity updates, including individual step updates. Tracking and monitoring enables the development of metrics to provide meaningful information to management, to enable informed decision making, and optimize the management of their programs.

Status Options

Each Risk, Issues, and Opportunity has a lifecycle of its own, from conception to disposition. To assist with the management of individual Risks, Issues, and Opportunities, various status options are utilized. They are defined in Table 25. These options not only provide an understanding of the maturity of a Risk, Issue, or Opportunity, but also provide traceability between the Risk, Issue, and Opportunities and the Risk, Issue, and Opportunity Process. Figure 45 demonstrates the relationship between the maturity of the status and the Risk Process. During the lifecycle of a Risk, Issue, or Opportunity, not all status options may be utilized, but their order should not change.

Table 25: Risk, Issue, Opportunity Status Definitions

Risk, Issue, and Opportunity **Status**	**Definition**
Watch Item	A Risk, Issue, or Opportunity that includes the minimum set of information along with a trigger date to re-evaluate current status and maturity.(1)
Draft	A Risk, Issue, or Opportunity that includes the minimum set of information through full maturity, prior to manager's endorsement.(1)
Proposed	A Draft Risk, Issue, or Opportunity that is ready for manager's endorsement. (2)
Pending	A Proposed Risk, Issue, or Opportunity that is awaiting RMB approval. (2)
Approved	A Risk, Issue, or Opportunity that has been approved by the RMB.
Not Approved	A Risk, Issue, or Opportunity that has not been approved by the RMB.
Disposition Ready	An Approved Risk, Issue, or Opportunity that is awaiting RMB decision for disposition. (2)
Closed	An Approved Risk, Issue, or Opportunity that has been found to be overcome by events, transferred outside the organization, or found to be duplicate.
Retired	An Approved Risk, Issue, or Opportunity that has not experienced its Impact and no further action is pursued.
Realized	An Approved Risk, Issue, or Opportunity that has experienced its Impact and no further action is pursued.

Note 1: While a Risk, Issue, or Opportunity can remain in a Watch Item status for an extended period, a Risk, Issue, or Opportunity in Draft status is intended to be quickly matured with the goal of obtaining management approval.
Note 2: Proposed, Pending and Disposition Ready are transition statuses that identify the need for management decisions. Risk, Issue, and Opportunities are not intended to remain in these statuses for an extended period of time.

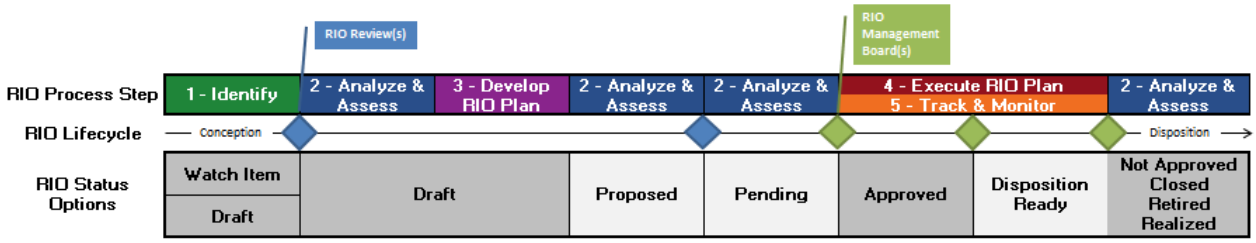


Figure 45: Risk, Issue, and Opportunity Status and Associated Process Phases

Risk, Issue, and Opportunity Reporting

The goal of Risk, Issue, and Opportunity Reporting is to establish clear communication with all stakeholders with special focus on providing a status on both new and actively managed Risk, Issue, and Opportunities. Risk, Issue, and Opportunity Reporting evaluates (vets and approves) all elements of a Risk, Issue, or Opportunity (e.g. statement, score, steps, etc.) in detail. Reporting provides a medium for all parties to discuss their thoughts on the subject. A distribution list and associated participation should be defined and documented to ensure appropriate involvement. Dissemination can be as simple as regular email distribution to team members or as formal as reoccurring meetings. Risk, Issue, and Opportunities change history should also be documented for historical (trend analysis) and audit purposes. A standard reporting format should be used to ensure consistency across the organization.

There are several methods that a program may use to report their risk activities to management. For example, a brief summary of all risks for a particular project can be displayed on an aggregate risk grid – also called a Probability Impact Diagram (PID) – as shown in Figure 46. A standard reporting format shall be used to facilitate integration of risk information across projects and programs. It is recommended that the RMP also indicate the extent of required supporting detail.

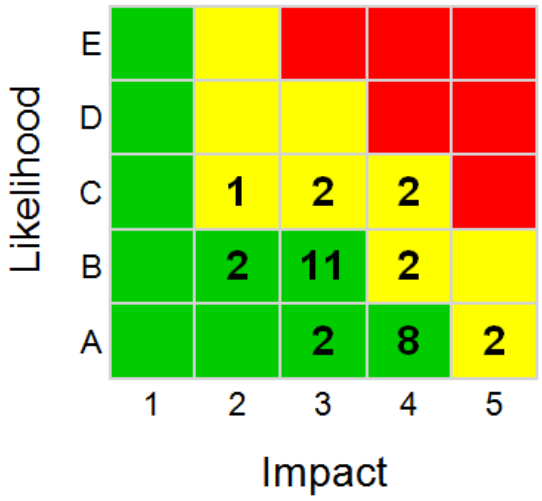


Figure 46: Probability Impact Diagram (PID) Example

It is recommended that the management visibility effort be focused on monitoring and tracking the effectiveness of the risk reduction decision. The impact of the risk on the program and the relevant *decision* are incorporated into the project schedule as risk mitigation actions. They are inserted into the program's Integrated Master Schedule. The lowest level tasks involved are flagged with the assessed

risk level; higher-level Work Breakdown Structure (WBS) tasks inherit the maximum risk level present in any subordinate task. Hence, review of the schedule at any level from summary tasks to lowest level tasks allows program management to maintain appropriate risk visibility and also allows "drill down" to increasing levels of detail as the schedule view is expanded.

OMB Reporting Requirements

Major FAA programs must submit yearly budget estimates with supporting justification for the investment in accordance with OMB Circular A-11. These submissions are provided as an "Exhibit 300" in a format prescribed by OMB. OMB uses risk as a factor to measure the health of investment programs based on the Exhibit 300 data. OMB requires that the risk-related data be presented in various sections of the Exhibit 300 as defined in Circular A-11. Examples where risk should be reflected may be found in the sections discussing life cycle cost estimates, program schedules, privacy, security, and the structuring of major acquisitions. In particular, the cost estimates and schedules for the investment should show how they have been adjusted for the risks associated with the investment. The OMB requirement is to provide objective evidence that all aspects of risk have been considered in managing FAA investments. OMB is looking for "an integrated process within an agency for planning, budgeting, procurement and management of the agency's portfolio of capital assets to achieve agency strategic goals and objectives with the lowest life-cycle cost **and least risk**." (Circular A-11, 2012). Please note that the OMB terminology discussion of "risk contained in risk management plans" (same reference) refers to risk mitigation plans as discussed in this section of the FAA SEM.

4.3.3 Outputs

Risk management efforts directly influence the decisions and progress of program or solution development. The principal outputs of the process are:

The primary outputs of the Risk Management Process are:

- Risk Management Plan
- Risk Register
- Aggregate Risk Grid (Probability Impact Diagram)
- Risk Metrics
- Risk Mitigation Plan Summary
- Risk Summary
- Risk Mitigation Plans

Risk management recommendations:

- Brief the Program Risk Summary, the Risk Mitigation Plan Summary, and the Program Risk Mitigation Progress charts at all regular program reviews
- Brief a complete status of a given risk when the risk is identified and immediately following the risk realization date, as management decisions are based on the above information
- Handle the Risk Mitigation Plans as an integral part of the program effort.

4.3.4 Considerations for System of Systems

Typically, FAA systems are composed of a number of interrelated systems that work together to achieve a common purpose, such as providing an operational capability. This System of Systems (SoS) approach introduces a number of risk management considerations that must be addressed:

- Risk management processes and tools employed by interfacing FAA organizations must be compatible and configured with data interchange in mind. It is preferred that a common tool, such as Active Risk Manager, be used by interfacing FAA organizations.
- Risks may be managed and owned by various levels of the FAA, including programs, portfolios, and the FAA Enterprise
- Risk mitigation may depend on resources, activities, and products spanning multiple programs and organizations
- Risk mitigation planning may require coordination between multiple programs and organizations
- Risks within one program or organization may be linked in a parent-child relationship between programs, portfolios, and the FAA Enterprise
- Risks may be transferred between program, portfolio, and enterprise levels if the risk can be more effectively handled at that level
- Risks may be escalated to a higher organizational level if mitigation of the risk requires authority and responsibility of the new level

Key to understanding the above considerations are the concept of risk linkage, depicted in Figure 47. The relationship between the levels of risk is critical for understanding risk management, scope, and mitigation. An integrated view results in relationships between risks, where one risk, and the mitigation of that risk, may relate to one or more additional risks, and the mitigation of those risks.

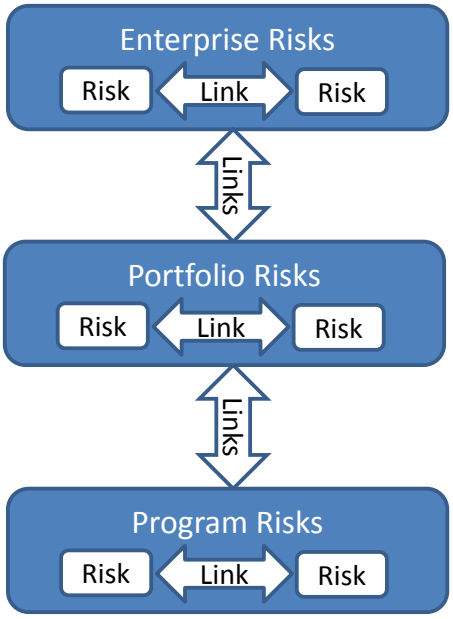


Figure 47: Risk Linkage

4.3.5 Risk, Issue, and Opportunity Management Tools/Outputs

The tools and outputs needed to implement this process include:

- Risk Management Plan
- *Risk, Issue, and Opportunity* Worksheets

A Risk, Issue, and Opportunity Worksheet may be used by programs to guide the practitioner through the first three tasks in the Risk, Issue, and Opportunity Management process: identify Risk, Issue, and Opportunities, analyze Risk, Issue, and Opportunities, and develop mitigation planning. When a Risk, Issue, and Opportunity mitigation plan has been prepared, management reviews and approves it based on criteria defined in the RMP.

- Likelihood and impact Scorecards
- Risk, Issue, and Opportunity Reports

  A listing of Risk, Issue, and Opportunity information associated with achieving program objectives. These registers can be used to monitor and track overall Risk, Issue, and Opportunity status within team meetings, program management reviews, and major program reviews. When a Risk, Issue, or Opportunity becomes approved by management it shall be incorporated into the register.

- Risk, Issue, and Opportunity Database Tool

  The use of a Risk, Issue, and Opportunity Management database tool supports commonality, integration, and increased efficiency. It provides management with a consistent reporting capability/format to support their various needs, and allows Risk, Issue, and Opportunity managers to efficiently manage Risk, Issue, and Opportunities on a day-to-day basis. There are several COTS database applications available for use, e.g. Active Risk Manager (ARM), Risk Radar, and Primavera. ARM has been selected by several FAA organizations for use as an integrated Risk, Issue, and Opportunity management tool and can be extended to additional users.

- Risk, Issue, and Opportunity Management Training

  Risk, Issue, and Opportunity training workshops should be oriented toward ensuring that all participants understand and act in compliance with the Risk, Issue, and Opportunity Management policies and procedures defined for the organization. The Risk, Issue, and Opportunity Manager has the responsibility to provide training, with assistance from SMEs, with the following tasks in mind:
  a. Identify the type and amount of training required to ensure that all participants in the Risk, Issue, and Opportunity Management process understand and comply with the policies and procedures defined in their RMP.
  b. Coordinate the development of in-house training modules with functional managers, and review and approve external training options.
  c. Develop training workshops

- Risk, Issue, and Opportunity Metrics

Additional Information

For sources of information used to generate content throughout this section, see References.

To learn more about the topics in this section, see Additional Tools and Reading Recommendations.

4.4 Configuration Management

Configuration Management (CM) is a management process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life. Configuration Management facilitates the process of documenting, validating, and verifying system performance and functional/physical attributes to preserve system integrity. Additionally, CM provides a structured process to identify, review, approve, document and implement changes to system attributes. Configuration management requirements, milestones and artifacts are required by AMS through documentation, reviews and decisions throughout the acquisition process.

Baseline establishment is imperative to Configuration Management. A baseline is an agreed-to description of the attributes of a product at a point in time that serves as a basis for defining change. Establishing and maintaining product baselines makes managing a system moving through the lifecycle much easier. Configuration Management keeps the inevitable changing of project artifacts under control by eliminating the confusion, and errors that result, from dealing with multiple versions of project artifacts as well as the issue of unauthorized changes to these artifacts.

Controlling changes to these baselines is the other aspect of CM. Configuration Control Boards (CCB) are formal decision-making bodies that are part of the FAA's governance structure. They support the functional and operational integrity of a baseline through establishment and enforcement of effective change management and control practices and processes.

Configuration Management occurs in every phase of the AMS lifecycle. It is an iterative process in that it provides a closed-loop process for managing change. System Engineers use the CM process for all SE products.

Objective: The Configuration Management Process establishes and maintains the integrity of all identified outputs of a project or process and makes them available to all concerned parties.

4.4.1 Inputs

The primary inputs to the CM process are described below:

1) **FAA Policy –** FAA Order 1800.66, "Configuration Management Policy" prescribes the requirements and details FAA CM processes and procedures. The Order governs the introduction of new products and services to the NAS, or any changes to existing products or services. This policy is a standalone document and is part of the FAA Acquisition Management System (AMS).

2) **Change Requests**

- **External Change Requests** are submitted by contractors, typically during development, to request changes to contractor-controlled baselines.
  - **Engineering Change Proposals (ECP).** An ECP manages developmental, allocated, and functional baselines prior to solution implementation. An ECP may be used by the contractor for the modification of systems hardware and software, and to manage allocated documents.
  - **Requests for Deviations and Waivers.** During product development or production, a contractor may need a requirements deviation or waiver. The contractor submits a request to deviate from (planned) or waive (unplanned) a specific requirement, as applicable. The contractor submits requests for deviation (RFD) or requests for waiver (RFW) to FAA. An RFD/RFW is generally temporary and is brought into compliance at a later time.
  - **Contractor Change Vehicles.** The contractor- or developer-approved CM plan documents (or "vehicles") that affect the change process.
  - **Memoranda of Understanding (MOU).** MOU is a documented agreement between FAA organizations or between FAA and an external organization when no formal

contractual relationship exists between the parties. MOUs serve as source data to be kept as part of the program documentation and used to drive, validate, and verify program activity as necessary during the CM process.

- **Internal Change Requests** submitted by parties within the FAA provide suggested changes to FAA-managed baselines. FAA uses NAS Change Proposals to accomplish this.
  - **NAS Change Proposal (NCP)** – The NCP is the coordination vehicle used internally to formally manage NAS baselines. Every NCP must consider any safety or security issues that the change could generate.

3) **Systems Engineering Management Plan (SEMP)**
   - **Configuration Management Plan**. Configuration Management Plan describes the CM strategy, implementation activities, and standard practices for performing CM for the project of interest.
   - **Work Breakdown Structure (WBS)**. The WBS provides a logical structure for developing the products that will be placed under CM. This structure assists CM in establishing the Configuration Items.
4) **Configuration Documents** support or describe a product or service and must be retained as program information**.** Some are approved through the NAS change process. Examples include**:**
   - Requirements (e.g., NAS-RD, PRD, SSD, IRD, ICD)
   - Validated tools and Reference Models
   - Test article and apparatus configuration
   - Design documents
   - Drawings
   - Technical instruction manuals
   - Maintenance handbooks
5) **Change Releases** notify that a change or modification occurred. Change release notes specify configuration items that were changed, the approval authority, and in some cases the installation or implementation date.
6) **Configuration Status Accounting Reports (CSAR) –** NAS CSARs are available through the FAA's automated CM support tools for the NAS change process and Master Configuration Index (MCI) or other program data sources. They provide the current status of configuration items or work products from Life Cycle Engineering to keep CM status current.

4.4.2 Configuration Management Process Elements

Configuration Management consists of the following steps:

12. Develop a CM Plan
13. Identify Configuration
14. Select Configuration Items
15. Establish and Maintain Baseline
16. Manage Approved Baseline Changes
17. Provide Configuration Status Accounting
18. Verify and Audit Configuration

19. Monitor Configuration Management Activities

Each of these activities is described in more depth below.

1) Develop a Configuration Management Plan. CM planning determines the resources for the CM activities throughout the lifecycle, establishes the mechanisms for performing the CM process, designates the responsibilities of the organizations performing the CM process, and ensures that control is extended to vendors and contractors during the equipment acquisition.

The Configuration Management Plan addresses these issues. A discussion of planning for CM appears in Section 4.1: Integrated Technical Management. Sample CM plan content may be found in FAA Order 1800.66. The CM plan ensures that the program and functional managers control the integrity and continuity of the requirements, design, engineering, and cost tradeoff decisions. The Configuration Management Plan is included in the SEMP for the project of interest, or as a standalone document.

At a minimum, a good Configuration Management Plan should do the following:

- Identify Stakeholders
- Identify and Gather CM process inputs
- Identify CM tool, when applicable
- Establish schedule for CM activities
- Establish Communication Plan with Stakeholders
- Establish a Configuration Control Board (CCB)
  - A CCB is the FAA-authorized forum for establishing configuration management baselines and for reviewing and acting upon changes to these baselines. A CCB supports the functional and operational integrity of a baseline through establishment and enforcement of effective change management and control practices and processes. Each CCB develops operating procedures according to its specific mission and needs. FAA Order 1800.66 provides requirements for developing and maintaining CCB charters and operating procedures.
- Establish CM Procurement Requirements
- Establish CM Procurement Strategy

2) Identify Configuration. Configuration identification is the systematic process of selecting product attributes, organizing associated information about the attributes, and stating those attributes. It includes assigning and applying unique identifiers for the product and its associated documentation, as well as maintaining document revision relationships to the product configurations. These attributes mature through each of the lifecycle phases and, at key milestones during those phases, are validated and incorporated into the baseline.

3) Select Configuration Items. A Configuration Item (CI) is an aggregation of hardware, software, or firmware that satisfies an end-use function and is designated for configuration management.

In accordance with agency or organizational policy or practices, each work product must have an assigned unique identifier so the SE can track CI using version or revision levels (including preliminary versions and drafts). File-naming conventions should be consistent and easily traceable to the product title.

Electronic files maintain individual files to allow traceability to historical records. Each new version or revision of a file must have its own unique identifier. SEs should maintain original files, rather than overwrite them. See FAA Order 1800.66, paragraph 3.3.2.5 Data Management, for detailed procedures.

4) Establish and Maintain Baseline – The progression of a product through its lifecycle appears as a series of baselines. Key product milestones provide a snapshot of the product configuration at

the respective lifecycle phase. Agreed upon and recorded definitions of CIs and their attributes is a baseline. They include specific versions of approved and released documents that serve as the basis for managing change. Because of the complexity of the NAS, FAA maintains an enterprise-level baseline and several other baselines established for an acquisition program. There are five baselines, each described below: Functional, Allocated, Product, Facility, and Operational.

- **Functional Baseline** – The functional baseline is the approved documentation describing the system's functional, performance, interoperability, and interface requirements and the verifications required to demonstrate achievement of those specified requirements. The functional baseline represents the functional requirements for a program and is the first formal program baseline to be established after concept exploration.
- **Allocated Baseline** – The allocated baseline is the approved documentation describing a CI's functional, performance, interoperability, and interface requirements that are allocated from the requirements of a system- or higher-level configuration item; interface requirements with interfacing configuration items; and the verifications required to confirm the achievement of those specified requirements. The allocated baseline represents the program's design requirements. This baseline is typically established after the System Requirements Review. The allocated baseline for FAA is the system and interface requirements that will be used for an acquisition program.
- **Product Baseline –** The product baseline is the configuration of the system or product being delivered to the customer. It consists of the combined performance/design documentation used in Configuration Identification for production/procurement. This documentation package incorporates the cumulative baseline documents describing a CI's functional, performance, interoperability, and interface requirements and the verifications required to confirm achievement of those specified requirements. It also includes additional design documentation, ranging from form and fit information about the proven design to a complete design disclosure package. The milestones for establishing the product baseline include the successful completion of the formal Functional Configuration Audit (FCA) and the Physical Configuration Audit (PCA).
- **Facility Baseline –** The facility baseline is the information needed to identify and control changes to end-state and as-built facility space drawings and critical power panel schedules. This baseline is an essential element of FAA planning for introducing NAS systems and subsystems. Establishment of a facility baseline is determined by assessing the impact of Capital Investment Plan projects as well as regionally and nationally initiated changes and improvements. Configuration management of facilities is described in the complementary documentation FAA-STD-058 and Order 1800.66.
- **Operational Baseline –** The operational baseline is the approved technical documentation representing installed operational hardware and software. This represents a product baseline adapted to local conditions. Operational baselines comprise the technical documentation that initially describes a delivered system. They also include changes to that delivered system that occur as a result of in-service modifications/improvements or as a result of the addition of FAA-developed documentation/tools. The operational baseline includes the product baseline and any subsequent changes to it. Operational baselines describe the system as deployed in the NAS.

Data Management – Data management is the preparation, approval, distribution, and storage/archiving of recorded information of any nature/type (administrative, managerial, financial, and technical) regardless of medium or characteristics. In the context of managing NAS products or systems, work products are not formally part of a product's configuration. Work products developed within the program/project requiring management's signature must undergo, at a minimum, coordination and version control. Work products associated with the managed program/project are identified, and requirements for managing changes to those

work products are established. Key work products are determined by the project leader and include AMS-mandated documents, contract documentation, and program plans. As with any CM activity, work product procedures should be documented and included in planning documentation to ensure consistency and quality of work products.

5) **Manage Approved Baseline Changes –** Configuration Control is the systematic process that ensures that changes to released configuration documentation are properly identified, documented, evaluated for impact, approved by an appropriate level of authority, incorporated, and verified. Modification of the product, product information, or associated interfacing products triggers a baseline change.

The FAA Configuration Control Board (CCB) authorizes the establishment of and subsequent changes to configuration baselines. The NAS CCB is the highest ranking CCB in FAA; it is established by the Joint Resources Council (JRC) or its designee. The NAS CCB has authority to charter subordinate CCBs as necessary. The service units typically update their CCB charter upon assignment of a NAS program.

The following steps must be completed in order to implement changes to approved baselines.

a) Identify and Describe Change – Applicable change vehicles document changes to Baselines. In the FAA, any person can identify a problem or suggest an improvement at any time during the product life cycle. Change vehicles state the problem or need for change, the proposed change, affected CI, cost, schedule for change implementation, interface impacts, risks and other factors necessary to assess the impact of the proposed change. The factors determining the type of change vehicle or the need for a change vehicle are the type of baseline, who is responsible for controlling the baseline, and the CM plan. Change vehicles are uniquely identified and require the identification of the baseline elements affected. For NAS baseline management, the FAA uses the NAS Change Proposal (NCP) form, which captures proposed changes to the form, fit or function of CIs identified as part of the NAS baseline. The NCP form and processing are completed using the National CM support tool as described in FAA Order 1800.66. Program Trouble Reports (PTR) and Hardware Discrepancy Reports (HDR) are the vehicles used, primarily by operational support personnel, to correct a defect or inconsistency without impacting any aspect of a baseline.

b) Evaluate Change – Coordination and review of changes embody the systematic approach for ensuring the validity, feasibility, and assessment of impacts of the change. Formal reviews capture each reviewer's name, organization, comments, date of review, and appropriate resolution of comments as applicable. Reviews must occur before adjudication. This approach includes reviewing changes to both formal and informal baselines.

c) Ensure Disposition of Change – Change disposition is the conclusion by the appropriate authority that the item submitted for approval is either suitable or unsuitable for implementation or release. CCBs serve as the forum for adjudicating proposed changes to formal baselines. Each CCB is an independent decision-making body within its prescribed level of authority. A CCB has decision authority for all changes affecting CIs assigned to the CCB.

d) Monitor Change Implementation – An important CM function is monitoring change implementation. This ensures the release and completion of installation or updates of approved changes. Change implementation is captured by closure of a Configuration Control Decision (CCD). The CCD is the official, legally binding FAA notification of CCB decisions and directives. The CCD identifies required actions and the organizations responsible for completing those actions. For example, CCD actions may include:

- Approval of physical incorporations of changes to affected hardware, software, or facilities
- Approval of technical evaluations, studies, or tests

- Directions for incorporation of changes in baseline documentation
- Field modification installation and tracking when changes are needed to facilities or operational equipment

6) **Provide Configuration Status Accounting (CSA) –** Configuration Status Accounting (CSA) is the systematic recording and reporting of system or product configuration status. CSA includes baseline change status and history for all items captured in the MCI, from establishing the initial baseline to the end of product service. CSA reports not only communicate status, but also support conduct of formal configuration audits when design documentation is not available or has not been updated to the current configuration. CSA information is automatically captured in the National CM support tools for the NCP process. The SE generates reports from these tools or performs CSA as required for all levels of CM across the life cycle.

   a) ***Capture change data –*** Capturing change data, typically by using the automated CM tool that was identified in the CM plan, enables recording and reporting of the status and history of baseline changes from initiation through implementation.

   b) ***Capture baseline configuration status –*** Baseline status updates occur as changes are proposed, reviewed, approved and implemented. When CSA reports are generated, a "snapshot" of the baseline is captured and can be used to conduct audits or reviews, or simply to check baseline information at that point in time. Baseline content evolves as the product goes through its lifecycle.

7) **Verify and Audit Configuration –** Conducting audits and quality checks ensures the integrity of the product. Functional and Physical Configuration Audits are examples of formal audit activities used to establish the product baseline. A functional configuration audit verifies that the product meets its functional and performance requirements and functions as intended. The physical configuration audit is a technical review of the CI to verify the "as-built" matches the approved baseline technical documentation. Quality checks, peer reviews, or internal audits of work products are informal means for documenting and managing the quality and validity of informal organizational baselines

8) **Monitor Configuration Management Activities –** Monitoring CM activities typically refers to monitoring contractor CM activities during solution implementation. Contract Data Requirements Lists (CDRLs) and Data Item Descriptions (DIDs) are the primary means of ensuring that the contractor delivers what is required and that those deliverables are satisfactory. The contractor's CM plan or other lower level programmatic agreements are also used to monitor CM activities and related processes.

4.4.3 Outputs

The primary outputs of the Configuration Management process are:

- **Baselines and Updated Baselines** – Baselines established during the CM process and any changes to these baselines. Types of baselines include: Functional, Allocated, Product, Facility, and Operational Baseline.
- **Baseline Changes** – Baseline changes are captured and available to all CM users, decision-makers and stakeholders on demand.
- **Configuration Status Accounting Reports (CSAR)** – Configuration status accounting reports (CSAR) provide the current status of CI configuration items, work products, or change status. CSARs are provided on demand or at scheduled intervals.

Additional Information

For sources of information used to generate content throughout this section, see References.

To learn more about the topics in this section, see Additional Tools and Reading Recommendations.

4.5 Systems Engineering Information Management

The FAA uses the term Information Management in a different manner than the INCOSE Systems Engineering Handbook and other international standards for systems engineering. Therefore the FAA SEM will use the term Systems Engineering Information Management, shortened to SEIM, to name the systems engineering activities that are simply called Information Management by INCOSE.

The SEIM process collects, manages, stores, and distributes all information pertaining to a particular project. This process also manages enterprise level information that is needed during the project. SEIM applies various policies, procedures, and information technology to maintain the integrity of all information generated during a project's lifecycle. The SEIM process ensures that the correct information is available when needed. The process provides accurate and secure project information in a timely manner that can be used as both inputs and outputs of the other systems engineering processes. The process supports many of the iterations of the Integrated Technical Management process

Information is any and all processed data and data is defined as raw, unorganized facts. Information is data that has been organized so that it has meaning and value to the recipient. Information can be stored and communicated, and it might include customer information, proprietary information, and/or protected and unprotected intellectual property. The recipient interprets the meaning and draws conclusions and implications. Information exists in many forms and varies project to project. During the lifecycle, much information is used, generated, and collected. The value of this information will depend greatly on its users. As projects and systems become more complex, so will their information and data. It will be critical to have a systematic way to keep all the information and data organized and managed throughout the lifecycle. For the purpose of this manual, information and data will be used interchangeably.

4.5.1 Inputs

An input to the process is information that the SEIM process needs that provides directions; is the basis for or otherwise drives SEIM process activities; or requires action through one or more SEIM tasks.

The primary inputs to the SEIM process fall into three categories: Information Management, Information Products, and Information Requests. Each is described below.

Systems Engineering Information Management Guidance

SEIM guidance refers to documentation with which the Information Management PDCA cycle activities must comply. PDCA is introduced in Section 1.4. This includes any stipulations, restrictions, or instructions on how project information is to be acquired, maintained, and stored. Some Information Management guidance may even address who can and cannot gain access to certain project information. Some examples of SEIM guidance include:

- FAA policy, procedures, and orders
- Standards
- Program policy and procedures
- FAA and organizational agreements
- FAA legislation

Information Products

Information products are what the SEIM process will manage. The information products will depend on the scope of the project and will vary from project to project. The project manager and systems engineer will work together to determine a project's information needs. Information products can be any recorded information, regardless of the form or method of recording. This can include administrative, managerial, financial, contractual, and technical data. The information products will evolve as they move through the lifecycle and it will be imperative to successfully implement the information management process, to ensure that the information products remain current and up to date. Information products are the primary input to the SEIM process. Some examples of information products include:

- Concept of Operations (ConOps)
- Intellectual Property Documents
- SEMP, including the Integrated Technical Plans
- NAS Enterprise Architecture information and views
- Joint Resources Council (JRC) Secretariat submittals and JRC Records of Decision
- Screening Information Requests (SIR), vendor proposals, and Source Selection Protest files
- Specifications
- Contract Statement of Work
- Work Breakdown Structures
- Budgets
- Meeting Agendas and minutes
- Contract deliverables
- Knowledge Sharing Network (KSN) or equivalent, data sharing and productivity libraries, tools, and environments
- NAS operational information content
- Logistics documentation, drawings, COTS documents
- Accident investigation files
- Congressional correspondence
- Project management reporting tools
- Office of Management and Budget (OMB) / General Accountability Office (GAO) / Department of Transportation (DOT) Inspector General (IG) correspondence and initial audit findings
- Specialty process documentation (risk, security, safety, logistics, design, test, operational operating authority, etc.)

Information Requests

Distributing project information and data is part of the SEIM process and information will often be distributed upon request. Information requests can come from a variety of sources and the fulfillment of these requests will be at the judgment of the project manager. Keeping a thorough record of information requests and a record of release of controlled information will help maintain the integrity of the project.

4.5.2 Systems Engineering Information Management Process Elements

4.5.2.1 Plan Systems Engineering Information Management

SEIM provides the foundation for the acquisition, management, storage, and distribution of project information throughout the lifecycle; therefore, adequate planning is necessary.

The SEIM plan outlines how information will be acquired, managed, distributed, and stored. This plan is part of the project SEMP. The SEIM Plan should be tailored accordingly to fit the information needs for that project of interest.

At a minimum, a good SEIM Plan should do the following:

- Identify valid sources of information
- Identify valid list of project stakeholders
- Define information format requirements

- Define information storage and retention requirements
- Define information access privileges
- Define information security requirements
- Allocate resources and schedule for acquiring, maintaining, transferring, distributing, and disposing of project information

4.5.2.2 Perform Systems Engineering Information Management

All process activities are conducted in compliance with the SEIM guidance available for that particular project, phase, and milestone. A project's information products are both inputs and outputs of this phase.

The SEIM Process activities are as follows:

- Acquire information products
- Validate information products
- Maintain information products
- Distribute information products
- Archive information products
- Retire information products, when applicable

These activities are described below:

Step 1: Acquire Information Products

Gathering the information that will be managed is the first step in performing SEIM. What, when, and how information will be acquired varies from project to project. A project's Systems Engineering Information strategy identifies information sources, restrictions, formats, security requirements, relevant guidance, and stakeholders. This ensures that credible, correct, and useful information is gathered on time without jeopardizing the information's integrity or violating any organizational, agency, or congressional policies, orders, or laws.

When the information is acquired or originated, it becomes an information product associated with a particular program. As stated earlier, an information product is recorded data of any nature, regardless of medium or characteristics. Most information products will be acquired electronically, although there may be some instances where information may need to be manually acquired.

Step 2: Validate Information Products

Often too much information is available with multiple versions of the same document, order, instruction, handbook, drawing, etc., which need to be filtered for the most current, or for a past baseline version, in effect at the time in question. For example, contracts that have had a succession of modifications to the requirements may need a rolling baseline set of attachments all marked-up to the current understanding, configuration, and ready to be issued again in the form of specification revisions. Validation of the version, contents, and parameters of old information products will require system engineering resources to keep frozen and working sets of marked up documents current.

Step 3: Maintain Information Products

After acquiring the information products, the next step is to maintain them as the project moves through the lifecycle. Information maintenance will depend greatly on the type of information product and the information needs of the identified stakeholders. The project manager and systems engineer will work together to determine how a project's information will be maintained as well as how often maintenance will be required. All of this information will be detailed in the project's SEIM plan. Proprietary, controlled, sensitive, secure, and other legal restrictions on data release must be afforded proper processing and due consideration.

Some common tasks in maintaining project information include:

- Storing information products for easy and expedited retrieval
- Prioritizing and reviewing information products to ensure, at a minimum, that they are accurate, relevant, valid, and complete
- Protecting information products from security threats and privacy breaches
- Protecting information products against hazards or natural disasters (*i.e.* fire, flood, earthquakes)
- Destroying working papers, old or duplicate versions, and expired data at the proper time

Step 4: Distribute Information Products

One of the major goals of SEIM is to make sure that information is available when it is needed. Having a formal process to manage a project's information among contributors, reviewers, and approvers, allows for information to be distributed more easily and quickly.

Generally, project information will be distributed upon request, and as needed. Each request will be reviewed and evaluated to determine the requested information availability, validity, and the information privileges of the requester. Not all information requests will be granted. The access rights of the requester as well as information sensitivity, security, and availability are just a few of the reasons that can cause an information request to be denied.

The SEIM plan will detail how and when information products will be distributed or denied in response to information requests for the project and to ensure compliance with the necessary SEIM guidance.

Step 5: Archive Information Products

During the lifecycle, many information products are generated and some will need long-term storage, therefore becoming "project archive" information products. Keeping a record of past information products will be useful in identifying lessons learned and best practices. Additionally, having historical data available will be a valuable resource in identifying project risks.

Which information products are archived will be at the discretion of the project manager and systems engineer. A project's SEIM Plan will outline the archival requirements of the information products and the schedule for when they are archived.

Properly protecting and preserving archived information products will also be very important to this step. A majority of the archived information products will be unique and so it will be necessary to keep the information in a safe place.

Step 6: Retire Information Products

As a project moves through the life cycle, some information products will no longer be relevant, accurate, necessary or valid and will need to be destroyed or discarded. This step will be completed on an ad hoc basis as the need arises. The project manager, along with the systems engineer, will work together to determine which information products are retired.

Even though the retiring information is thought to be no longer needed, there are still security, privacy, and legal issues that may need to be addressed. Information products must be discarded in compliance with applicable SEIM guidance, security, and privacy requirements. Improperly disposing of information products could threaten the integrity of the other information products not being retired.

After performing SEIM, information products should be shared with team members in a centralized location, where they can be protected, regularly maintained, available when needed, and retired when deemed no longer relevant.

4.5.2.3 Review and Update Systems Engineering Information Management Activities

The information management processes may need to be periodically reviewed and updated. Some SEIM checklist items to consider include:

- Date and availability of SEIM guidance. Checking to make sure all the information activities are conducted according to most recent version of organizational policies, laws, and orders will ensure the information products' integrity.
- Validity of information sources. Acquiring information products from valid sources will save money and reduce the information products accessibility to security threats and privacy breeches.
- Access rights and privileges of information requesters. Ensuring that the correct people have access to the correct information will prove beneficial in the areas of information accuracy, security, and validity.
- Information products storage locations. Storing information products in safe and secure locations benefits the entire Information Management process.
- The SEIM Plan must also be updated to reflect changes to guidance or procedures.

4.5.3 Outputs

The primary outputs of the SEIM process are timely, secure, correct project data and information.

4.5.4 Tools

Some information technology tools that can help to maintain the integrity of information and assist in sharing information with authorized stakeholders include:

- DOORS: Primarily a requirements documentation tool. It is used to control versions, track changes to requirements, and ensure traceability.
- NAS EA Portal: A good source of information for enterprise-level architecture products and requirements. Guidance documents are available.
- Knowledge Sharing Network (KSN): An access-controlled repository for electronic documents.
- Documentum: Stores official versions of documents.
- System Architect (SA): Creates and edits architecture products. With proper controls on the databases, versions of the products can be maintained.

Additional Information

For sources of information used to generate content throughout this section, see References.

4.6 Decision Analysis

The Decision Analysis process is a means of assessing the various alternative outcomes of a decision in order to determine a preferred or optimal choice. Decision Analysis uses a variety of tools, methods, and procedures that inform a decision by identifying and assessing decision criteria and alternatives in order to provide a complete understanding of the outcomes. This process quantifies the benefits and consequences of selected alternatives in terms of metrics that trace to stakeholder expectations and overall project objectives. The Decision Analysis process provides a structured methodology for decision-making throughout the system development lifecycle.

The Decision Analysis process and supporting tools aid in making decisions, analyzing trade-offs, evaluating alternatives, and performing trade or market studies. Systems engineers and other decision analyst use this process to inform the making of decisions that range from very high-level strategic decisions to more technical, lower-level decisions. Decision Analysis is beneficial for all of the formal decision gates during the AMS lifecycle but is most emphasized in the Investment Analysis decision gates where the FAA decides whether or not to allocate money to an alternative. Decision Analysis supports each systems engineering process by providing the preferred set of functions, requirements, or architecture through the analysis of design alternatives, system trade-offs, mission benefits and system lifecycle cost. A number of tools and techniques support the decision making process and provide a foundation in which to justify a decision. Included later in this section is a description of some of the more common methods.

In order to thoroughly inform a decision the Systems Engineer must work with key stakeholders, and analyst through the Integrated Multidisciplinary Team (IMT). The IMT works together to establish the need for the use of a formal decision process which triggers the Decision Analysis Process. They will also work together to tailor the process to the decision. The primary outputs of the Decision Analysis process are the recommendations for a selected alternative and the impacts of that selection.

4.6.1 Inputs

The inputs to the Decision Analysis process vary from project to project and greatly depend on the scope of the decision.

Decision Analysis governance refers to any and all documentation with which the Decision Analysis activities must comply. Decision Analysis governance may constrain alternative solution options, decision criteria, and in some cases define project budget and schedule. It is imperative to conduct the Decision Analysis activities in compliance with the available governance and guidance for that decision in order to reach the optimal decision. Some examples of Decision Analysis governance include:

- FAA policy, procedures, orders
- Standards
- Program policy and procedures
- FAA and organizational agreements
- FAA legislations
- FAA and Project SEMP
- Decision Analysis Plan

Because Decision Analysis occurs throughout the life cycle, the inputs may include any outputs from the systems engineering and technical management processes. However, the decision will use only a subset of the full list of inputs based on the position in the life cycle. Some common examples of Decision Analysis inputs include:

- Decision need
- Assumptions and constraints
- Identified unique alternatives

- User needs
- Concept of Operations
- Requirements documents
- Enterprise architecture
- Analysis criteria

4.6.2 Process Elements

Decision Analysis planning ensures that the best choice is selected when alternatives exist. Conducting upfront planning prevents the project manager from committing too early to a decision that may not be cost effective, meets all of the systems requirements, or contains unnecessary risk. Decision Analysis requires input from all member of the IMT with the objective of producing an optimum design. Developing a Decision Analysis plan is the major step required to plan for decision analysis.

4.6.2.1 Steps for Performing Decision Analysis

The Decision Analysis Plan may be found in the SEMP for the project of interest. The formality of the decision determines the rigor and level of detail for the following major tasks:

1. Develop Decision Analysis Plan
2. Identify and justify the need for the decision
3. Determine the scope and ground rules of the decision
4. Define evaluation criteria and weighting factors
5. Determine alternative solutions
6. Evaluate alternatives
7. Perform sensitivity analysis
8. Review results and form conclusions

Each step is described below.

Step 1: Develop a Decision Analysis Plan

The Decision Analysis Plan dictates how the decision analysis process activities will be implemented for a particular decision. The Decision Analysis Plan is included in the SEMP for the project of interest. More information on a SEMP is available in Section 4.1: Integrated Technical Management.

A Decision Analysis Plan addresses the following:

- What the team needs to document throughout the process
- Roles and responsibilities for decision making team
- Schedule determining when the decision maker needs to make a decision, when possible

Step 2: Identify and justify the need for the decision

Formal Decision Analysis can require a significant amount of resources and time depending on the complexity of the decision and the techniques used to make the decision. Because of this, it is important that there is a need for a formal decision and that the scope of the Decision Analysis properly aligns with the level of level of effort required to make the decision. Applying the decision analysis process improperly can cause major schedule delays and exceed the allotted budget. Identifying and justifying the need for a decision upfront reduces a project's susceptibility to technical, schedule and cost risks. Some reasons to make a decision and trigger the Decision Analysis process include the need to:

- Choose among alternative designs, implementation strategies, or solutions based on architecture, performance, and cost in order to meet stakeholder requirements

- Choose between development or COTS products for acquisition
- Select a supplier for service
- Document and justify the selection of a solution for a systems requirement
- Reduce risk

Step 3: Determine the scope and ground rules of the decision

After identifying the need for a decision, the next step is to understand the goals and scope of that decision. In order to define the goals and scope the engineer must first gather the decision inputs. Maintaining communication with the decision stakeholders is crucial to completing this step successfully as understanding the viewpoints of all the decision stakeholders will clearly define the key issues.

Properly identifying the problem statement and achieving consensus with all decision stakeholders on the needed decision saves significant time in the overall process by making the completion of subsequent tasks much easier. As part of determining the scope, decision analysis requires the decision team to identify all assumptions, simplifications, or constraints involved in analyzing the decision. The outputs of decision analysis can vary drastically with the use of different assumptions or constraints. This makes identifying and evaluating assumptions and constraints important for framing the scope.

The scope also needs to identify the tool, technique, or method that the team will use to analyze and evaluate the alternatives. The selected tool, technique, or method needs to provide, as an output, the same level of detail that the decision requires. If too little fidelity is available in the technique, the information for making the decision will be incomplete and if too much fidelity is provided by the technique, the technique requires more resources and time than necessary. There are a large number of tools, techniques, and methods available to the systems engineer for decision analysis, each with their own benefits and limitations. Because of this, the FAA does not prescribe the use of any one particular tool or recommend one over the other. This manual describes some of the more common and helpful tools for consideration and includes information on when their use provides the most benefit. The most common tools are often the easiest to use and the ones that make the most assumptions, limiting their usefulness for complex decisions. Because of this, prior to using any of the techniques described in subsequent sections, the systems engineers should familiarize themselves with the assumptions and limitations of each technique in order to make sure decisions are consistent with reality.

Step 4: Define evaluation criteria and weighting factors

Evaluation criteria and weight factors establish quantitative metrics that enable the judging of the selected alternatives. They provide the basis for assessing alternative solutions. Evaluation criteria define “what matters” and weight factors define “how much” a criterion matters regarding a specific decision. Defining evaluation criteria and their associated weights require considerable engineering judgment and interaction with the decision stakeholders. The Decision Analysis strategy for the decision of interest should identify the relevant stakeholders.

The systems engineers will work with the decision stakeholders to identify the correct evaluation criteria for the decision of interest. Typically, requirements decompose into evaluation criteria. Although not always possible, evaluation criteria should be measurable; in the instances where a criterion is qualitative and not measurable the decision analysis plan should establish a quantitative value for quality. Expressing evaluation criteria in quantifiable terms allows the engineer to analyze the alternatives and compare them against each other in a faster and more efficient manner. Cost, reliability, supportability, testability, and compatibility are a few examples of common criteria that the Decision Analysis process uses to evaluate alternatives; additionally, each decision will include more criteria specific to the decision. The following types of evaluation criteria are applicable to a wide range of decisions:

- Development cost
- Lifecycle cost
- Requirements compliance
- Functional criteria
- Performance criteria
- Operational criteria
- Programmatic criteria
- Technical risk

- Budget risk
- Schedule risk
- Reliability, Maintainability, and Availability
- System safety
- Human Factors
- Electromagnetic environmental effects
- Hazardous materials
- Operational complexity
- Industry assessment
- System maturity
- Test and development support tools
- Familiarity with candidate hardware and software
- Logistics support

Assigning weighting factors can be a difficult task and is very subjective. Not all evaluation criteria will have the same importance and the same criterion can have several different weighting factors depending on the scope of the decision. The systems engineer will be responsible for assigning the correct weightings to the selected evaluation criteria, while the project manager will be responsible for ensuring consensus among all the decision stakeholders. There is no standard format for assigning weighting factors but the most common techniques are a simple 1 to 10 rank (with 10 identifying the most important evaluation criteria), and a percentage approach in which each criterion is a weighted as a percentage of the entire list of criteria. Quality Function Deployment (QFD) and the Prioritization Matrix are some additional tools that aid in the definition of the evaluation criteria and weighting factors. Critical Performance Requirements (CPR) can also play a key role both as an input and an output for evaluating criteria and weighting factors. By establishing a weighting factor for the shortfalls or users functional need the systems engineer can use evaluation criteria to determine how well each requirement meets each function. The requirements with the highest scores are the most critical. CPRs can also be used as evaluation criteria that already contain a weighting factor through their designation as critical.

Helpful Tools

- **Prioritization Matrix**

  Description: The Prioritization Matrix is an easy technique to establish weights for the design criteria. The Prioritization Matrix measures one criterion against all of the remaining criteria by asking if the criterion is significantly less important, less important, equally important, more important, or significantly more important than the other criteria. The technique produces a numerical score by assigning the following values:

  Significantly More Important = 5

  More Important = 3

  Equal Importance = 1

  Less Important = 1/3

  Significantly Less Important = 1/5

  The sum of the values for one criterion produces the overall score. Once each criterion has an overall score, the sum of all of the overall values produces a total that allows for the percentage calculation. The agreement of the IMT and the stakeholders is important for properly assigning the importance values and producing the weighted percentage.

  Best used when:

  - No definition of priorities exists from customer needs or QFD

- **Quality Function Deployment**

  Description: QFD is a methodology that gathers, interprets, and deploys the stakeholders' operational needs and requirements in developing a product or service. The primary objective of QFD is to eliminate three major problems: difficulty in gathering and interpreting stakeholder's requirements; loss of information; and different individuals and functions using varying

interpretations of the same requirements. QFD provides a Decision Analysis tool that screens alternatives using weighted selection criteria. QFD requires teamwork among the IMT to address requirements from multiple perspectives. QFD elicitation should involve the customer, representatives from the product development and support functions, and suppliers.

Best used when:

- Stakeholder requirements are vague, ambiguous, or self-contradictory
- Multiple disciplines are involved in the collection and interpretation of the requirements
- Lack of an obvious feasible solution
- Cost and/or risk appear to be unacceptably high

Step 5: Determine alternative solutions

The next step is to determine a set of viable alternatives for the decision of interest. Trade publications, prospective bidders for service contractors, technical staff, stakeholders, and managers, as appropriate, are helpful resources in developing a set of alternatives that may potentially achieve the goals and objectives of the system (e.g., architecture, designs, and COTS products).

When numerous possible alternatives exist, a detailed analysis of each one may not be cost effective and the most beneficial use of resources; therefore the engineer should use down-selecting until the results provide significant distinction between the alternatives. On average, four to six alternatives provides enough representation of the solutions and distinction from each alternative. If there is not enough distinction from six alternatives, the systems engineer should then perform a sensitivity analysis. Identifying high-risk alternatives and those alternatives with questionable feasibility or high lifecycle cost helps reduce the number of alternatives to be analyzed. Screening the alternatives against the evaluation criteria also eliminates alternative candidates. Therefore, the systems engineer should identify and eliminate those options that do not meet the essential evaluation criteria as early as possible. It is important to document all alternatives considered.

Helpful Tools

- **Morphological Matrix**

  Description: The Morphological Matrix is a technique for exploring all the possible alternatives to a decision. When using this technique the IMT brainstorms all architectural element alternatives that meet each of the functional criteria of the project. By selecting one architectural element alternative as a design choice per each functional criterion the process develops one system level alternative for evaluation. While this technique theoretically will produce thousands of system alternatives most are not viable since component incompatibilities will limit the number of available choices.

  Best used when:

  - Brainstorming unique technical alternatives
  - Defining functional or system architectures

- **Baseline Reference Method or Pugh Matrix**

  Description: The baseline reference method (also known as a Pugh Matrix) involves evaluating alternative solutions against a baseline, legacy design, or other reference using the selected evaluation criteria. This method requires a team effort of all disciplines participating in the decision. Each alternative is given a rating and all decision stakeholders must agree on the rating assigned to each candidate solution. Generally, the symbology “(+)” is used for an alternative clearly better than the baseline, “(-)” for alternatives clearly worse than the baseline, “(S)” for same as baseline, and “(U)” for unacceptable as the baseline.

  Best used when:

  - Selecting architectural elements or components to define alternatives

- Assessing the benefits of technical refreshes and system improvements

Step 6: Evaluate alternatives

The systems engineer further analyzes the set of alternatives identified in Step 4 to determine how well they satisfy the evaluation criteria selected in Step 3. The scope of the decision, the evaluation criteria, and the available resources all contribute to the selection of an evaluation technique and method for a particular decision.

The evaluation tool appropriate for the decision of interest analyzes the alternative solutions to quantify the outcome variables by computing estimates of system effectiveness, underlying system performance or technical attributes, and project cost.

The following actions are best practices when evaluating candidate solutions:

- Perform a detailed evaluation of all approved viable alternatives. Record any problems or questions and, if a weighted matrix method is used, finish scoring without reference to weights or flags.
- Evaluate the alternative approaches relative to the evaluation criteria.
- Identify any alternatives with high-weighted score that narrowly failed the pass/fail criteria. Discuss these alternatives with the stakeholders.
- Evaluate cost factors separately from the remaining evaluation criteria throughout the Decision Analysis process.

In some cases, none of the candidate solutions may satisfy all the evaluation criteria. In such cases, it may be necessary to relax one or more of the criteria, investigate additional alternatives, or report to the stakeholder that the results produced no entirely acceptable solution.

Helpful Tools

- **Relative Rank Method**

  Description: The relative rank method evaluates each alternative against the selected criteria and establishes a ranking for each criterion. Weighting of the criteria is defined by category, while the alternative solutions are graded in their appropriate columns according to scaling factors over a range of 0 to 4. The average ranking within each category is multiplied by the criteria weighting to determine a score. Scores are summed across the criteria.

  Best used when:

  - There are a large number of decision criteria covering multiple disciplines
  - There are relatively few alternatives
  - Evaluation Criteria are qualitative
  - The decision is a lower level decision with little impact on cost and schedule, and is low risk

- **Technique for the Order of Prioritization by Similarity to Ideal Solution (TOPSIS)**

  Description: TOPSIS is similar to the Relative Rank Method, but expands on the concept by evaluating alternatives against a positive and negative “ideal.” This fixes the limitation of the Relative Rank Method where often the alternative that performs the best against the highest priority criterion has the highest score regardless of the alternatives score against other criteria. TOPSIS defines the ideal solution by selecting the value of the highest performing alternative for each criterion to establish a hypothetical perfect (positive ideal) and worst case (negative ideal) alternative. The alternatives are evaluated by how close their score is to the positive ideal and how far it is from the negative ideal. The alternative that has the largest distance from the negative ideal and the shortest distance from the positive ideal is the best solution. TOPSIS can also compare direct performance values and does not require a qualitative assessment of the alternative’s performance assuming the criterion is measurable. Note that TOPSIS is a more

mathematically complex technique and will be more time consuming than the Relative Rank Method and may not provide a different result.

Best used when:

- There are a large number of decision criteria covering multiple disciplines
- There are relatively few alternatives
- Overall performance of the alternative is important
- Evaluation Criteria are primarily quantitative or performance based
- The decision is a lower level decision with little impact on cost and schedule, and is low risk

- **Decision Trees**

  Description: Decision Trees are a method of analyzing all of the possible outcomes from a decision. The decision initially branches in to the alternatives. The systems engineer analyzes each alternative by assessing the probability that the alternative will produce a certain value. These probabilities are the chance events or risks associated with the alternative. Note that chance events can also produce subsequent chance events thus decision trees are often very large diagrams with a high number of branches. The alternative with the highest probability of achieving the highest value (known as having the highest utility) is the preferred alternative. Decision trees provide for a significantly more thorough and consistent decision making process over other methods, but may be difficult or time consuming to develop properly.

  Best used when:

  - There is a thorough understanding of the uncertainty or risk associated with a chance event
  - The decision requires a high level of consistency in order to produce the optimal choice
  - The decision is primarily value based
  - (Note: the most common definition for value in the FAA is cost per benefit ratio but value is a generic term and allows for other definitions)

- **Influence Diagrams**

  Description: Influence diagrams are models that contain all of the possible outcomes for a decision, similar to decision trees. Influence diagrams use four components to model the decision process, decision variables, chance events, calculated value, and objective value or utility. Decision variables are inputs that the IMT defines prior to performing the analysis; these are typically the starting point of the Influence diagram. Chance Events are the probability scenarios of an event occurring. They are typically inputs and only influence other elements. Calculated values are all intermediate calculations involved in the decision process. Calculations process an input in a finite repeatable way based on physical or mathematical models. The objective value is the overall output of the influence diagram and represents the overall goal of the decision. Similarly to the decision tree the objective value in the FAA will most likely be cost per benefit ratio. In order to show the interactions of the components, a lined arrow connects on component that influences another. Note that influence arrows cannot create a circular process because an objective value will not exist. Influence diagrams provide for an equally thorough and consistent process as decision trees and are also an improvement on the other techniques.

  Best used when:

  - Decision trees become too complex to analyze
  - The decision is primarily value-based
  - The decision requires a high level of consistency in order to produce the optimal choice
  - Mathematical or physical models exist for chance event and calculated values

- **Modeling and Simulation for Decision Analysis**

Description: Models and simulations are standard engineering tools that represent the key functions of a system and the interactions between the functions and the interactions with the outside environment. The defining feature of any model is its purpose. In general, a model represents how the system operates in its environment. An excellent guideline to follow is to select the least complex model that provides the most visibility into the problem. Simulation is an entire discipline that aids systems engineering decisions by exploring the decision outcomes and their effect on system design, system operation, and system cost. With simulations the trade-off between work required and the quality of the results is highly coupled. When a simulation better represents real world results it produces a more accurate understanding of the decision but requires significantly larger development and run times. When using simulation for decision analysis it is important that the systems engineer defines the scope and required result of the simulation accurately and that the simulation is feasible within the time frame for system development. It is best to use simulations for decision analysis when the decision is complex and has many unknown variables that cannot fit into one of the other methods described earlier with the exception of influence diagrams. Influence diagrams establish a structure for a decision model for simulation by establishing the interactions and shared parameters between engineering design choices, risk analysis chance events, financial cost models, and financial and technical benefits. A full description of Modeling and Simulation for decision analysis is outside the scope of this manual, but additional information is available on modeling and simulation in the Cross-Cutting Technical Methods Section in this document and online at the FAA Library and through NASA's Aviation Systems Division.

Step 7: Perform sensitivity analysis

Performing a sensitivity analysis after evaluating the alternative solutions may be necessary. Sensitivity analysis is useful when the candidate solutions are nearly equivalent in scoring.

Recommended actions for performing a sensitivity analysis include the following:

- Analyze all alternatives to determine if the differences between the scores are truly significant and if minor variations in the raw scores and weights might affect the selection. Reference any questions or problems noted by the evaluators. For each alternative, including any solution that is compliant based on redefined pass/fail criteria; determine if any weighted score or total for a group of related weighted scores is sensitive to variation of weights or scores.
- Evaluate the effect on weighed scores of varying weights as group decisions on weights introduce bias. Reevaluating weights with the IMT can produce different results.
- Evaluate the sensitivity of weighted scores to variation of scores. If a number of evaluators have evaluated the alternatives against a given criterion, the range of scores recorded provides useful guidance for such variation.
- Record the ranges of scores and weights. Compute the upper and lower bound for weight scores. Document the data in a matrix corresponding to the score and the weighted score matrices.
- Determine if any of the variations are large enough to require special attention by inspecting or using a suitable statistical test.
- Evaluate the effect on weighted scores total, including or excluding criteria flagged as non-critical.

Common outcomes of the sensitivity analysis and review of results include the following:

- Case 1: One alternative emerges as the optimal choice
- Case 2: More than one alternative is acceptable
- Case 3: No single, entirely satisfactory alternative is found

Case 3 is the most difficult to resolve. A review of evaluation criteria may indicate that the analysis identified no satisfactory alternative. In this case, the IMT is required to use engineering judgment and

discussions with the stakeholder to define additional alternatives or to accept a less-than-optimal alternative.

Step 8: Review results and form conclusions

This step typically presents one alternative as the best option after the completion of the evaluation and analysis all of the applicable candidate solutions. The decision analysis team then makes recommendations to the defined FAA decision authority, which makes the final decision. A Decision Report should document all assumptions, constraints, and changes from the baselines used during the analysis.

Validate Decision Analysis Activities: The Decision Analysis process provides the information and analysis to ensure the selection of the optimal solution when alternatives exist. Therefore, checking to make sure the decision is based on accurate information is imperative to obtaining meaningful results.

Decision Analysis validation checklist:

- Accuracy, relevance, and validity of decision information
- Accuracy, relevance, and validity of decision guidance
- Evaluation Methods: Check to ensure correct application and performance of the methods
- Analysis Reports
- Evaluation Criteria

4.6.3 Outputs

Decision Report: A decision report is the documented outcome of the decision analysis process. The report details the decision results and provides traceability to previous lifecycle decisions. The decision report documents the decision-making process that provided the preferred alternative over the others, the assumptions, and the decision outcome from the decision maker. The IMT should develop a standard format for the decision report that satisfies the project needs for consistency and ease of use. At a minimum, a decision report should include the following:

- Clear problem statement
- Identification of affected requirements
- Ground rules and assumptions
- Decision criteria
- Resource requirements statement to accomplish the decision
- Schedule to accomplish (actual and proposed)
- Evaluation of all potential solutions and screening matrix
- Comparisons of alternatives using decision criteria
- Technical recommendations from the decision analysis team
- Documentation of any decision leading to the final technical recommendation

Additional Information

For sources of information used to generate content throughout this section, see References.

4.7 Verification and Validation

Verification and Validation (V&V) are distinct, disciplined approaches to assessing work products, product components, and products throughout the life cycle of a solution. A *product* is defined to be "the final or end system, service, facility, or operational change that is intended for delivery to a customer or end user." A *product component* is a lower-level part, element, or module of the product. A *work product* represents, defines, or directs product development, and is typically a document of some type. Note: in this section, the words "system" and "product" are frequently used in place of the more generic "solution".

Verification and validation are defined as follows:

- **Verification** ensures that selected work products, product components, and products meet specified requirements and standards. Verification is inherently an incremental process since it occurs throughout the development of work products and products. Simply stated, verification ensures that the product is "built right."
- **Validation** is the process of incrementally ensuring that a work product, product component, or product will fulfill its specified purpose when placed in any aspect of its intended environment. Work products are validated on the basis of being the best predictors of how well the product and product components will satisfy user needs. Work product validation also reduces the level of risk to the program, as it occurs relatively early in the solution life cycle. Validation essentially guarantees that "the right product is built."

The primary purpose of V&V is to ensure a quality product is built that is operationally effective and suitable. Executed properly, the processes detect and correct defects as early as possible to minimize or eliminate their propagation to future activities. For additional guidance in the application of V&V policies, refer to the FAA AMS Lifecycle Verification and Validation Guidelines document, hereafter referred to as the V&V Guidelines. Guidance documents for individual AMS life cycle phases also have sections detailing the type of V&V performed in each one.

4.7.1 V&V in the Product Life Cycle

Verification and validation activities occur throughout the AMS life cycle to support the FAA in creating the best possible products for the agency and its stakeholders. As an essential aspect of systems engineering, V&V is frequently depicted in a "V" diagram that helps clarify the processes. Finally, comprehensive planning is of critical importance to successful V&V. These topics are covered in the following sections.

AMS Life Cycle

V&V supports all AMS decision points and ensures that the developed product – which may be systems, services, operational changes, or facilities – will fulfill mission needs and satisfy all requirements. V&V should be factored into the entrance criteria for these major decisions. Quality V&V reporting supports informed decision-making and risk management, and contributes to the overall effectiveness and efficiency of the program. For more information on the specific SE products and artifacts supporting the AMS decision points, see Section 2.2: Phases of the AMS Lifecycle Management Process. While both verification and validation activities occur throughout the AMS life cycle, Figure 48 depicts the primary emphasis of V&V between the major decision points. Note that these are not the *only* V&V tasks that occur at these points in the life cycle.

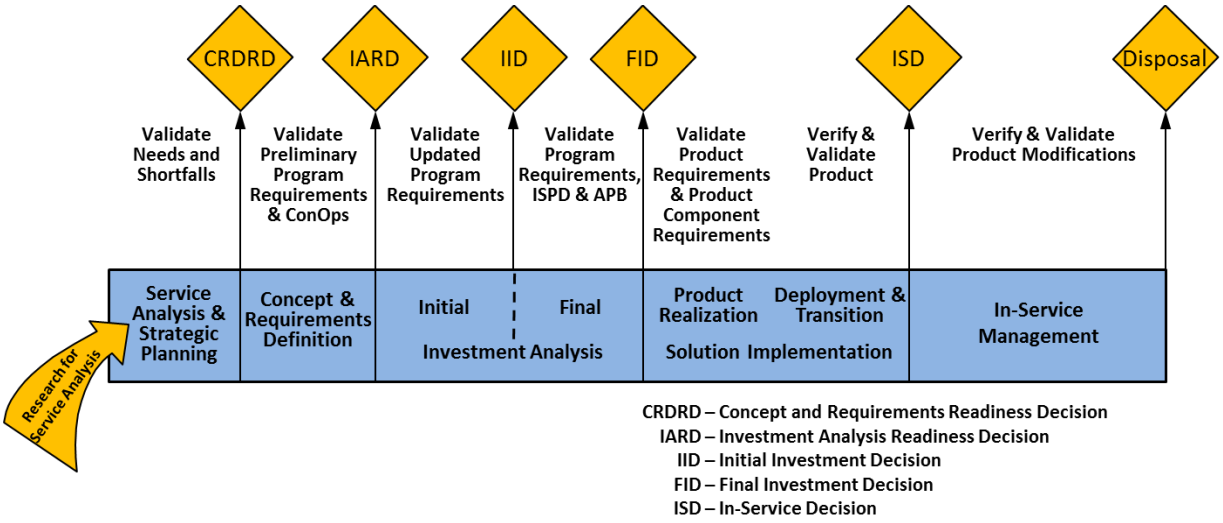


Figure 48: AMS Lifecycle Primary V&V Activities

The systems engineer is involved in all V&V activities, although the role and extent may vary depending on the activity. For instance, systems engineering is primarily responsible for the V&V of concepts and requirements during the earlier phases. The responsible service organization has a more significant function in the V&V of the design, and the Test and Evaluation (T&E) practitioner will guide the system testing during Solution Implementation.

For further detail on V&V activities within the AMS life cycle, see Section 3 of the V&V Guidelines. Further guidance may be found in the V&V sections of the guidance documentation on Service Analysis and Strategic Planning, CRD, and Investment Analysis.

The "V" Diagram

In the V&V process, a given work product, product component, or product is validated or verified against criteria identified in a work product in a previous step of the process. Each work product then becomes the basis for V&V of future work products, product components, and products. To graphically reinforce the point of the last paragraph, Figure 49 illustrates how the V&V process is employed by the FAA throughout a solution's life cycle. Initially, on the left side of the "V", V&V is performed primarily by systems engineers and almost exclusively upon work products such as concept documentation, requirements, and architectures. On the right side of the "V" diagram, one typically finds SE personnel supporting T&E teams. The focus during the Solution Implementation phase and beyond is verifying product components and products against requirements.

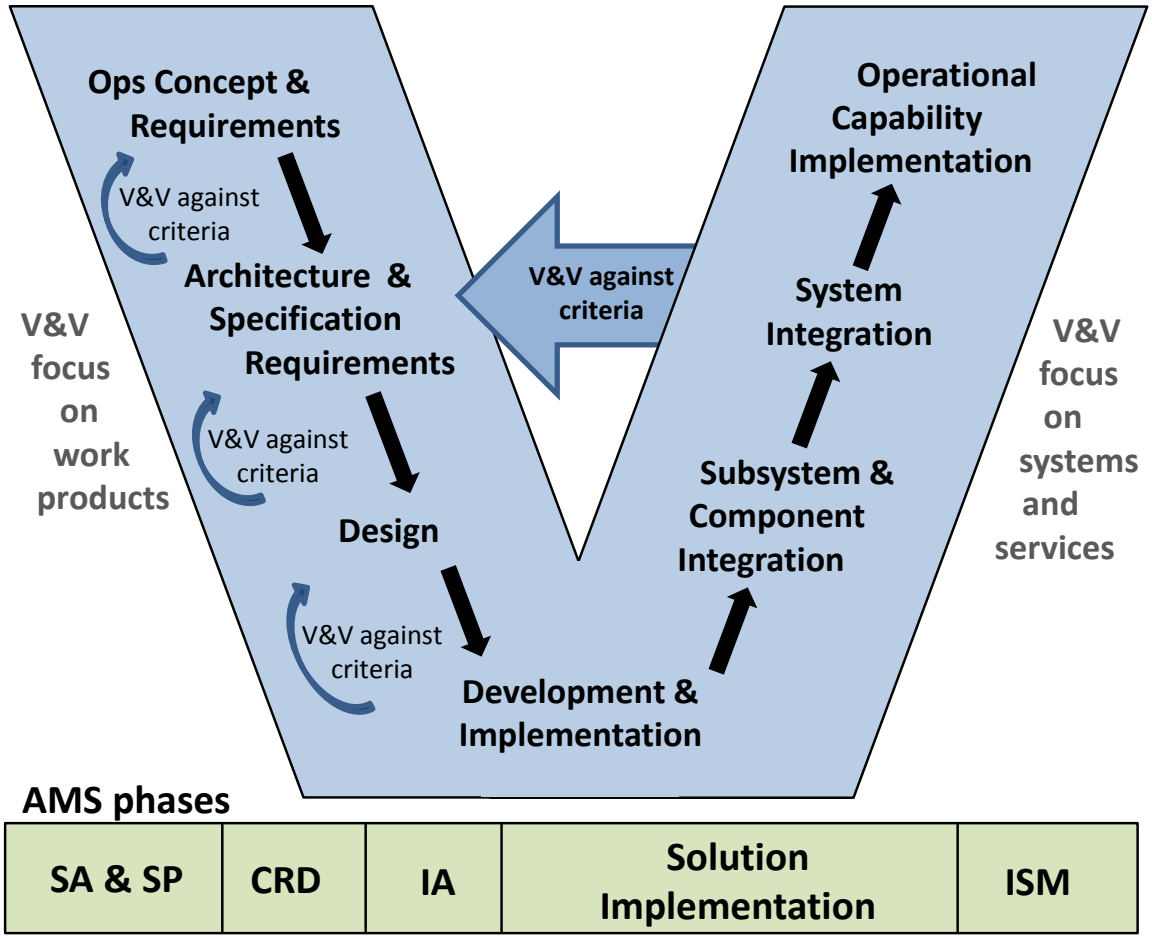


Figure 49: Systems Engineering "V" Model

Test and Evaluation

T&E is divided into three major activities; Development Test (DT), Operational Test (OT), and Independent Operational Assessment (IOA). DT supports the objectives of verification, ensuring the tested product or product component meets all specified technical and performance requirements. DT also verifies that the product is fully integrated and stable, and has no adverse effects on the rest of the NAS. OT and IOA support the objectives of validation by ensuring that major product components and the product are operationally effective, suitable for use in the NAS, and the NAS infrastructure is ready to accept the product. For details on the FAA T&E activities, refer to the FAA Test and Evaluation Process Guidelines (T&E Guidelines) or the Air Traffic Organization (ATO) NextGen and Operations Planning Services Test and Evaluation Handbook (T&E Handbook). The T&E Guidelines and Handbook complement one another and should be referenced together.

V&V Planning and Reporting

Careful planning and reporting of V&V activities is essential to reducing the risk of defects in any aspect of a solution. Planning for V&V well in advance of decision points helps to avoid schedule delays. V&V planning and reporting is required for all investment initiatives and should be formally incorporated into program planning documents and life cycle phase entrance criteria. These planning documents can include, but are not limited to:

- CRD Plan
- Initial Investment Analysis Plan

- Final Investment Analysis Plan
- Implementation Strategy and Planning Document (ISPD)
- Test and Evaluation Master Plan (TEMP)
- System Engineering Management Plan (SEMP)
- Quality Assurance Plan

As one example, V&V applied against program planning documentation may uncover inconsistencies within the document and its predecessor documents which could lead to increased risk, increased cost, and schedule delays. For more information on technical planning see Section 4.1: Integrated Technical Management, or the T&E Handbook.

In guiding SE activities, verification planning is typically contained in the SEMP. The plan includes the context, purpose, nature, and scope for each verification action. It also includes the Verification Requirements Traceability Matrix (VRTM) to use as a checklist during specific test planning and to ensure that all specifications and requirements trace back to a validated need or operational scenario. In addition, the plan identifies the product and product components along with their verification methods, which may be included as part of the VRTM and the TEMP. For more details on product verification planning, including the development of a TEMP and VRTM, see the T&E Handbook. In addition, Section 8.2: Appendix B: Integrated Technical Management Details contains information on the content and outline for the SEMP, Verification Plan, and other supporting documents.

The following guidelines are essential to properly reporting the results of V&V activities:

- V&V events must be documented and the corresponding documentation must be controlled and archived to ensure that historical records are kept
- V&V reporting should take into account that specific decision-making events and risk management will be based on the information contained in the report
- V&V reporting on the quality of work products should identify how well the work product supports development of an operationally effective and suitable end product
- V&V reporting of the results of test and evaluation activities (contained in final test reports) should identify how well the product or product component is built and to what degree it fulfills operational needs
- V&V reporting should take into account that subsequent work products, product components, and products can be premised off the information contained in the report

Table 26 shows a sample traceability matrix that may be used for verifying requirements.

Table 26: Traceability Matrix for Verification

Requirement ID	Description	Verification Method	Test Plan (name of DT plan)	Remarks
3.1.1.1 Aircraft ID	[*Requirement text*]	Test		
3.1.1.2 System Alignment		Demo		
3.1.1.4 Receive Time		Analysis		

4.7.2 Verification Process

The verification process ensures that work products are developed correctly. It also ensures that products and product components have been built correctly according to the requirements and specifications delineated in supporting work products. *Work products* are verified against criteria in policies, standards, and templates that define their content and format. As an example, a Preliminary Program Requirements Document is verified against the approved FAA Program Requirements Document template. Additionally, one may verify individual requirements against FAA guidance such as the Handbook for Writing Program Requirements, currently being developed by ANG-B1, NAS Requirements Services. An abbreviated version of this guidance material is also found in Section 3.3: Requirements Analysis. The process of work product verification is described further in the V&V Guidelines document and is not further elaborated here.

The *product* verification process ensures that the realized solution has satisfied the program requirements and that the solution is ready for validation. A fully verified solution is able to demonstrate that it satisfies:

- Requirements – functional, performance, allocated, derived, interface
- Architectures
- System specifications
- Design constraints
- Applicable standards

The verification process supports solution evolution during all phases of its lifecycle, from concept definition through product acceptance and in-service operation. It is a basic product development practice to verify that all requirements and specifications are satisfied. This principle does not imply that a test is required for every requirement, but it does imply the need to conduct a valid form of verification at an appropriate level for the given requirement. As requirements are developed, systems engineers must ensure that they are captured in a traceability matrix, such as the Verification Requirements Traceability Matrix (VRTM) described and shown previously.

The methods available for verification depend on whether it's a work product, product component, or product being verified. *All methods, however, can be grouped into the following basic categories: Inspection, Analysis, Test, and Demonstration*.

Verification Methods for Work Products

- Peer reviews
- Audits
- Checklists

Verification Methods for Products and Product Components

- Inspections
- Peer reviews
- Audits
- Checklists
- Analyses
- Testing
- Demonstrations
- Simulations
- Accreditation

A given product or work product may be verified through a combination of methods, if additional completeness or confirmation is required, for example. These methods are called out in the Verification Plan sections of the applicable work products listed previously.

Verification activities are grouped into three distinct phases: planning, verification, and documentation. Planning includes determining the resources required, the sequence and timing of activities, the documentation to be produced, and the assessment criteria. The results of verification are documented in the Verification Plans as discussed previously. The documentation phase ensures that findings are recorded, organized, and made available to appropriate stakeholders.

The activities that occur in these phases are described in more detail in the T&E Guidelines and T&E Handbook, in addition to the AMS policy material located at the FAST website.

4.7.3 Validation Process

The validation process demonstrates that a work product, product or product component is fit for its purpose and satisfies the stakeholder and service needs. Validation of work products ensures they support the development of an operationally effective and suitable end product. Product and product component validation ensures the final integrated product is operationally effective and suitable to end users and maintainers. As the systems engineer guides the evolution of the product requirements, validation ensures those requirements accurately reflect the stakeholder and service needs.

Successful requirements validation is often more challenging than verification – it requires much time and discipline to trace back and ensure that all needs are accurately addressed and confirm that the identified requirements are justified, relevant, and logically correct in terms of the anticipated operating environment. To achieve its objectives, validation activities are performed as early as possible in the acquisition life cycle.

The ConOps depicts operational scenarios and stakeholder expectations – while these are essentially preliminary requirements for a system or capability, they then can serve as validation criteria for subsequent products. The NAS Enterprise Architecture (EA) is a major source of validation criteria, as it defines the operational and technical framework for all capital assets of the FAA and describes current and target architectures. In return, the EA can be updated and refined based on the results of V&V. Requirements validation follows the development of program requirements; this aspect of validation precedes the solution design. Since these requirements are hierarchical in nature and developed in increasing detail as the lifecycle progresses, validation is an iterative process. As each level of requirements is developed they are validated by ensuring correct traceability to the previous levels and to EA documentation.

A significant role of the general SE process is ensuring that requirements have been sufficiently vetted and corrected before any solution development occurs. At each stage, the validation process provides increasing confidence in the program requirements and helps to ensure resources are not wasted on developing solutions for unnecessary requirements.

Validation Criteria

Many work products may be used as criteria for validation activities. This includes, but is not limited to the following:

- Enterprise Architecture
- NextGen Segment Implementation Plan
- Destination 2025
- Solution ConOps
- NAS Requirements Documents
- Program Requirements Documents – Preliminary, Initial, Final

- Critical Performance Requirements
- Functional Architecture
- Investment Analysis assessments
- Business Case
- Implementation Strategy and Planning Document

Many of the same methods used for verification can also be employed for validation.

Validation Methods

- Inspections
- Peer reviews
- Audits
- Checklists
- Analyses
- Testing
- Demonstrations
- Modeling and simulations
- Walk-throughs or dry runs
- Functional presentations
- User surveys or questionnaires
- Discussions with users

4.7.4 Verification and Validation Tools

There are several dedicated tools available to assist in managing the relationships between requirements, requirement validity, and verification methods. The selection of tools should ensure that the data is transportable and able to be integrated with other related SE results. A list of tools that may be used to facilitate this process is available on the International Council on System Engineering Web site (www.incose.org). Smaller projects may successfully manage these relationships with a simple spreadsheet or database application instead of a dedicated tool. Refer to Section 3.3.4.3 for more information on requirements management tools.

Additional Information

For sources of information used to generate content throughout this section, see References.

To learn more about the topics in this section, see Additional Tools and Reading Recommendations

.

5 Specialty Engineering

5.1 Reliability, Maintainability, and Availability (RMA) Engineering

This section provides guidance to facilitate, manage, and coordinate Reliability, Maintainability, and Availability (RMA) efforts, to ensure operationally acceptable RMA characteristics in fielded systems. SEM RMA Engineering is based on the FAA RMA Handbook (FAA-HDBK-006A) which includes the rationale for the RMA Engineering approach and explains the process in more detail. Section 3 of the handbook includes definitions of RMA engineering terms and parameters and provides background and context for the RMA Engineering discussions that follow. Handbook Appendices provide sample requirements and supporting analytical material.

The purpose of this section is to assist FAA Service Units and acquisition managers in the preparation of the RMA sections of procurement packages for major system acquisitions. The affected documents include System-Level Specifications (SLS), Statements of Work (SOW), Information for Proposal Preparation (IFPP) documents, and associated Data Item Descriptions (DID).

5.1.1 Definition

RMA Engineering applies engineering and management principles, criteria, and techniques to optimize the RMA performance of a system within the program's operational and programmatic constraints throughout the system lifecycle.

Reliability

Reliability is the ability of a system to perform as designed in an operational environment over time without failure. System reliability is commonly measured by Failure Rate and Mean Time between Failure (MTBF). These parameters are defined in Figure 50 and Figure 51.

$$\text{Failure Rate, } (\lambda) = \frac{\text{Number of failures}}{\text{Total operating hours}}$$

Figure 50: Failure Rate calculation

Failure rate (λ) represents the instantaneous failure rate, or the number of times the event is expected to happen in a given period of time. Mean Time between Failures, as represented by the symbol Theta (θ); is the Mean Life, or the average lifetimes of all items under consideration.

$$\text{MTBF, } \theta = 1 / \lambda = \frac{\text{Total operating hours}}{\text{Number of failures}}$$

Figure 51: Mean Time Between Failure calculation

Most FAA specifications for repairable or replaceable systems use Mean Time between Failures (MTBF). FAA's primary goal is safety, and increasing systems reliability is vital to the support of this goal. Systems reliability then supports Maintainability and Supportability, reducing operational costs and maintaining safety goals.

There are essentially two ways to accomplish this goal: Start with designing High Reliability systems, or optimize logistics resources to allow decreased Maintainability and Supportability. Reliability and Maintainability are some of the design parameters that must be considered. These two parameters are often trade-off in other to meet a higher-level requirement such as Availability. Refer to the RMA Handbook, for more detailed information.

Maintainability

Maintainability is measured by an item's ability to be retained in a specified condition through scheduled maintenance, or restored to a specified condition through proper repair.

Maintainability evolves from a series of statements and illustrations defining the input criteria to which the system should be designed. It evolves into a description of the planned levels of maintenance, major functions accomplished at each level, organizational responsibilities, basic support policies, design criteria associated with the support elements such examples include; built-in-test versus external testing, and personnel skill-level requirements, effectiveness criteria and anticipated maintenance environment requirements. Preliminary maintenance concept is developed during conceptual system design, and thereafter continuously updated in order to provide the desired influence on the mainstream system design and development. This system maintenance concept should address the question of "How will the system be supported, where, and for how long?"

Mean Time to Repair (MTTR) is a basic measure of maintainability and is defined as the total time required to diagnose a failure, isolate the failed component, replace the component, and return the system to operational status. The MTTR is an inherent system design characteristic. Traditionally, this characteristic represents an average of the times needed to diagnose, remove, and replace the various component types in a system. In effect, it is a measure of how easy it is to access malfunctioning equipment's failed components in combination with the effectiveness of diagnostics and built-in test equipment to detect and isolate the failure and the actions needed to return the equipment to service. The MTTR for a piece of equipment is related to the reliability (failure rate) of the various components comprising the equipment and the time to replace each of them.

For information systems, the Mean Time to Restore Service (MTTRS) is often used. It includes times for software reloading and system restart times in addition to the equipment repair time.

Availability

Availability is the probability that a system or part of a system may be operational during any randomly selected instant of time or, alternatively, the fraction of the total available operating time that the system or part is operational. Measured as a probability, availability may be defined in several ways, which allows a variety of issues to be addressed appropriately, including:

- **Inherent Availability (A_i)** – The maximum theoretical availability within the capabilities of the system or part. Computations of this construct consider only hardware elements and they assume perfect failure coverage, an ideal support environment, and no software or power failures. Scheduled downtime is not included in the Inherent Availability measure. Ai is an inherent design characteristic of a system that is independent of how the system is actually operated and maintained in a real-world environment.
- **Equipment and Service Availability (A_{es})** – Includes all sources of down time associated with unscheduled outages, including logistics and administrative delays, but excludes scheduled downtime. A_{es} is an operational performance measure for deployed systems and is monitored by the National Airspace Reporting System (NAPRS) for all reportable facilities and services.
- **Operational Availability (A_{op})** – The availability including all sources of downtime, both scheduled and unscheduled. A_{op} is an operational measure for deployed systems that is monitored by NAPRS.

Relationship between Reliability, Maintainability, and Availability

Inherent Availability can be derived from the required reliability and maintainability parameters according the formula in Figure 52:

$$A_i = \frac{MTBF}{MTBF + MTTR}$$

Figure 52: Inherent Availability calculation

The FAA uses availability as an operational performance metric for deployed systems by dividing the total time that the system or service is available in an interval by the total time in the interval. Operational availability combines the reliability performance of the operational system with the performance of maintenance personnel responsible for restoring service (following an interruption) into a single performance measure.

Availability can be useful as:

- A high-level planning tool for assessing architecture alternatives
- A tool for performing reliability and maintainability tradeoff analyses for logistics and Lifecycle Cost studies
- An operational performance metric for deployed systems

Availability is *not* appropriate for inclusion in contractual requirements as a primary specification for highly reliable systems. Availability is a gross oversimplification when applied to complex, software-intensive, fault-tolerant, information systems built from commercial, off-the-shelf hardware (See Section 3.3: Requirements Analysis for further discussion of RMA). Reasons why availability is not appropriate as the primary RMA requirement for modern digital systems include:

- **Availability implies that reliability and maintainability can be traded off.** Consider two automation systems, one having a predicted restart time of 3 minutes and a predicted MTBF of 5000 hours, and the other having a predicted 3-hour restart time and a predicted MTBF of 34 years. Both have a predicted availability of .99999, but the operational impact of failures would be vastly different. Moreover, while restart times are readily verifiable, MTBF predictions of 34 years are not credible and cannot be verified. Trading off actual restart times with problematic reliability predictions is unacceptable.
- **Availability cannot be predicted with enough accuracy to be useful.** Although the inherent availability of the hardware architecture can be predicted by straightforward combinatorial probability models, the primary determinate of the availability of software-intensive fault-tolerant systems is the effectiveness of the fault detection and recovery software. Since this effectiveness is dependent upon the effects of undiscovered defects in the software, it is virtually impossible to predict availability with any credibility before the software has been developed.
- **Contractual compliance with availability requirements cannot be verified.** It is impractical to conduct a statistically valid demonstration of the availability required by systems. To achieve a statistically valid result, the duration of the availability demonstration test would have to exceed the expected lifetime of the system. Moreover, it is virtually impossible to conduct a static demonstration of the system availability; software sourced problems may be ongoing and corrected and decisions will need to be made concerning which failures are relevant and how much of the resulting downtime is to be included in the availability calculation. Many of these factors are beyond the contractor's ability to control.

For these reasons, availability does not meet the SEM guidelines for good requirements. For more information, see the RMA Handbook, Section 5.2.3, and this manual, Section 3.2: Functional Analysis.

The primary causes of unscheduled service interruptions in modern information systems are latent software defects and excessive maintenance delays in restoring or replacing failed spare equipment, not hardware failures. Restoration times may be more dependent on computer restart times than hardware replacement times.

5.1.2 Employing RMA Engineering

Unlike most government agencies, where safety is simply a design constraint to attempt to prevent unintended consequences that could cause injury to persons or the environment, FAA's *primary* mission is safety. For this reason, RMA Engineering in FAA is closely related to both system safety engineering and risk management. Safety and efficiency are the primary considerations in the RMA Handbook's top-down allocation of availability requirements to FAA systems.

The purpose of the RMA section of the SEM is not to tell contractors how to build reliable hardware, but to provide guidance to FAA RMA engineers and acquisition managers on how to address many issues. Among these are: architectural issues, system-level RMA specifications, procurement package preparation, contractor proposal evaluations, design development monitoring, and the establishment of design validation and reliability growth criteria. Reliability, Maintainability, and Availability directly impact both operational capability and lifecycle costs and, therefore, are important considerations in any systems engineering effort.

The RMA characteristics of FAA systems are uniquely important because they can directly affect the ability to perform the agency's mission. Interruptions of critical services provided to air traffic specialists can adversely affect the efficiency of air traffic movement as controllers invoke manual procedures to maintain safety. However, during the transition interval from normal capacity operation to reduced capacity operation, safety hazards can exist as controllers increase separation and clear out the airspace until a steady state is reached. Figure 53 illustrates the transition to a reduced-capacity state and the hazard interval during the transition. The shaded triangle illustrates the interval in which safety hazard risk may increase. In most cases, this interval is non-existent or negligible and the only issue is the effect of the interruption on efficiency.

Some interruptions may have only nominal impacts nationwide, while others may result in critical, nationwide disruption of service. An example of an interruption with a potentially critical effect on efficiency but a negligible effect on safety is the loss of the capability to process flight data. On the other hand, loss of surveillance data or voice communications can result in a critical safety hazard until controllers are able to reduce traffic density and increase separation. Once a service has been identified as critical to providing safe separation of aircraft, an independent backup for the service must be provided to reduce the risk to acceptable levels.

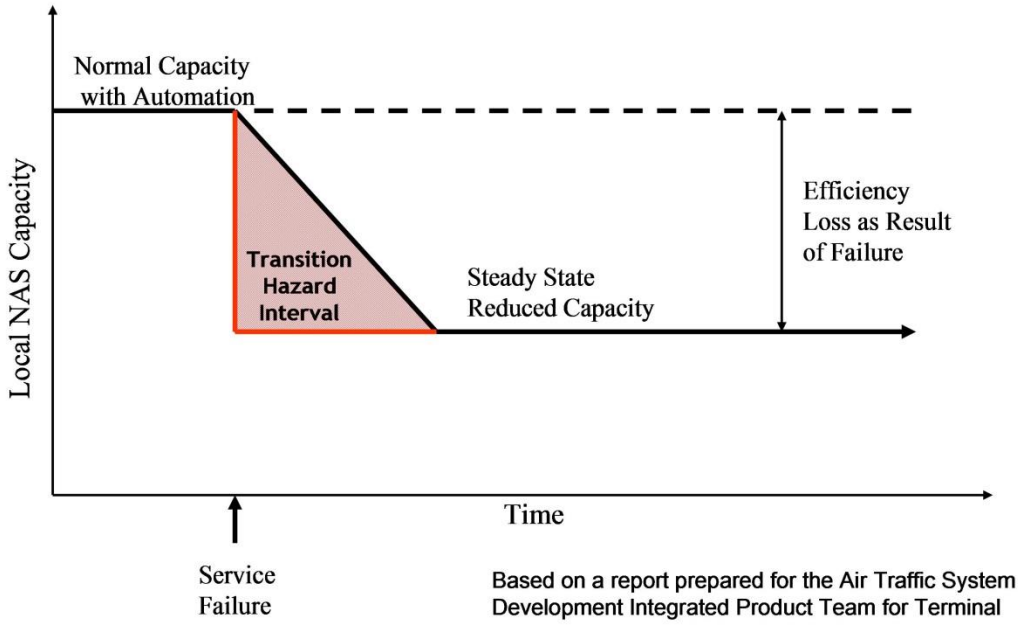


Figure 53: Effect of Service Interruptions on NAS Capacity

5.1.3 Inputs

Inputs to the RMA Engineering process include:

- FAA Policy and Standards
- NAS Enterprise Architecture
- NAS Requirements
- Systems Engineering Management Plan (SEMP)
- Program Requirements
- Functional Analysis
- Physical Architecture
- Contractor Technical Interchange Meetings and briefings
- Contractor Data Item Deliverables

RMA for FAA Systems

For the purposes of RMA, there are at least three categories of FAA systems: Information Systems, Remote and Distributed Systems, and Infrastructure Systems. Each category has different attributes that dictate unique treatment when specifying RMA requirements.

Information Systems

These are characterized and allocated by the NAS-Level RMA requirements. Information systems involve software-intensive air traffic control automation and communications capabilities. They have stringent availability requirements and, as a consequence of the large amounts of custom software that must be developed for them, entail significant cost and schedule risks. These programs provide the most critical operational services and have the most visibility. For these reasons, it is appropriate that they be given the most attention.

Remote and Distributed Systems

These are characterized by equipment such as sensors that "fan-in" to an information subsystem or services that "fan-out" from an information subsystem to a number of display workstations. These subsystems achieve the necessary overall availability through their reliance upon techniques such as diversity and overlapping coverage tailored to meet specific regional considerations. The subsystems are very robust because failures of individual elements only *degrade* the overall capability of the subsystem. It is not appropriate to attempt a "top-down" allocation of availability to these subsystems. Availability is a binary "up or down" measure that does not appropriately characterize subsystems that consist of multiple independent elements. To allocate availability to these elements requires making arbitrary "r of n" failure definitions, *e.g.*, 49 of 50 radars must be up for the surveillance subsystem to be up. If only 48 radars are operational, the entire surveillance subsystem is considered to be down. This does not reflect operational reality and can lead to unrealistic availability allocations. The availability requirements for the individual elements comprising these subsystems are best determined by life-cycle cost considerations, and acquisition managers' knowledge of achievable levels of reliability for the particular element in question. The overall operational suitability of the subsystem is best achieved by the judgment of subject matter experts in determining the number and placement of subsystem elements, not by an artificial and arbitrary mathematical allocation.

Infrastructure Systems

The infrastructure systems category refers to systems such as power systems, or heating, ventilation, and air conditioning (HVAC) systems that are required to support the equipment comprising the Service Threads. These systems typically violate the independent failure assumption underlying RMA calculations, as they can directly cause failures in the systems they support. Therefore, top-down allocations of availability requirements are not appropriate for these systems. Instead, FAA needs to develop a well-defined set of standard configurations that are consistent with the availability requirements of the Service Threads they support. The Service Threads are based on the National Airspace Performance Reporting System (NAPRS) services defined in FAA Order 6040.15. They represent "end-user" services delivered to air traffic specialists, and are essentially a reliability block diagram containing all of the "sensor to glass" equipment required to provide the service to the end-user.

RMA requirements are provided to satisfy the following objectives:

- Provide a bridge between user needs and System-Level Specifications
- Establish a common framework upon which to justify future additions and deletions of requirements
- Provide uniformity and consistency of requirements across procured systems, promoting common understanding among the specifying engineers and the development contractors
- Establish and maintain a baseline for validation and improvement of the RMA characteristics of fielded systems

•

5.1.4 RMA Process Tasks

RMA Engineering follows the specific process tasks described in Figure 54.

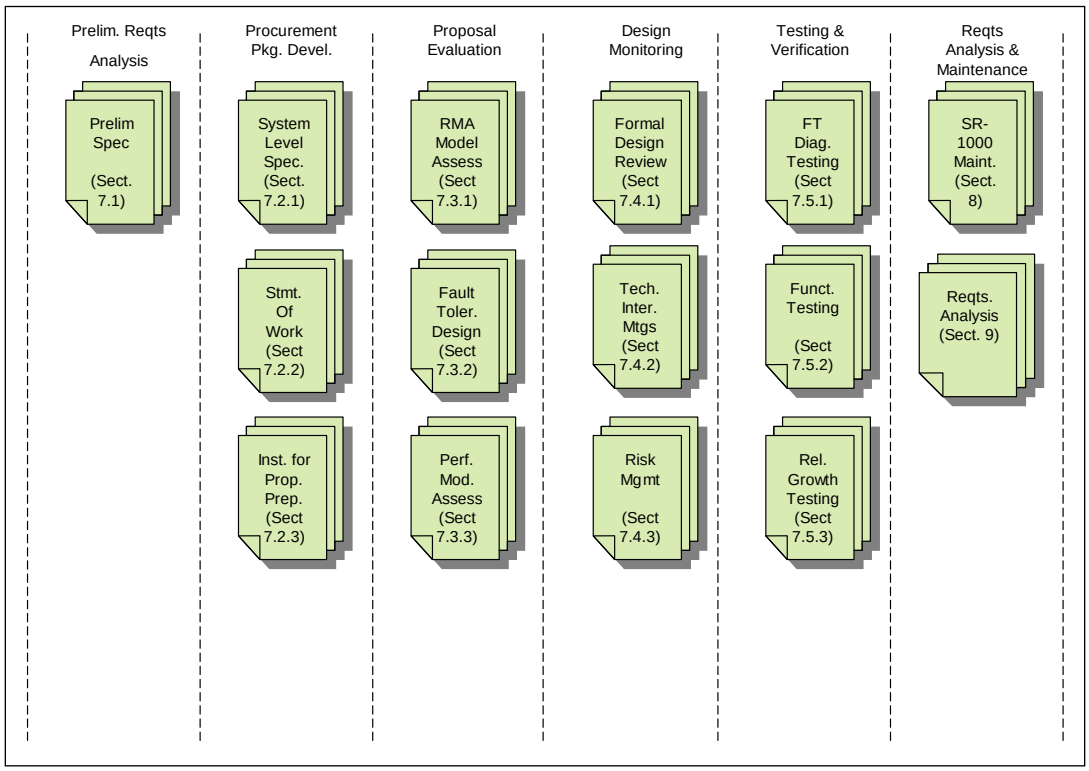


Figure 54: RMA Process Tasks

The figure depicts the relationship of the six RMA process tasks. The process task flow is from left to right and follows the acquisition process flow. Each step in a process task is keyed to the section of the RMA Handbook that describes the document to be produced.

Task 1: Preliminary Requirements Analysis

The primary objective of the preliminary requirements analysis task is to build a “bridge” between Enterprise-Level requirements and the procurement specifications for the tangible systems that will implement the requirements. The Service Threads are essentially a reliability block diagram containing all of the “sensor to glass” equipment required to provide the service to the end-user.

The process of allocating the availability requirements associated with NAS architecture capabilities to Service Threads is maintained in the RMA Handbook. This allocation is updated with the maintenance of the RMA Handbook, SEM, and requirements documents as the NAS evolves. The handbook describes the detailed methodology used to perform the Preliminary Requirements Analysis Task. (For more details, see the RMA Handbook, Section 7.1.) A traceability matrix specifies the relationship between the NAS architecture capabilities and the Service Threads. This matrix is a predecessor to the Operational Activity to Systems Function Traceability matrix (SV-5) in the NAS Enterprise Architecture Framework, where the NAS capabilities correspond to the Operational activities (OV-5) and the Service Threads are equivalent to the Systems Functions (SV-4).

Three levels of criticality, known as Service Thread Loss Severity Categories (STLSC), are associated with the interruption of the service provided by a service thread with an allocated

availability requirement established for each. Reliability and Maintainability requirements were established for the systems contained in a service thread, consistent with the allocated service thread availability.

The three STLSCs are:

- **Essential** – Service Thread loss could be accommodated by reducing capacity without compromising safety, with only a localized impact on NAS efficiency. (A = .9999)
- **Efficiency-Critical** – Service Thread loss could be accommodated by reducing capacity with economic impact on NAS efficiency without compromising safety, but the resulting effect might have a localized or system-wide impact. (A = .99999)
- **Safety-Critical** – Service Thread loss would present an unacceptable safety hazard during transition to reduced capacity operations. No single service thread can be permitted to provide a safety-critical service because there is no assurance that a single service thread can ever approach the required level of availability. Instead any proposed safety-critical thread *must* be decomposed into *two* independent service threads *each* having an availability of .99999.

Note: The current NAS has no single safety-critical service threads, because each instance of a safety-critical service has a primary service thread as well as a backup service thread. However, in every case the backup service thread was only added after the achieved availability of the primary service thread was proven to be inadequate. This requirement is designed to prevent the establishment of unachievable availability requirements from the outset.

Note also that the STLSCs differ from the traditional criticalities associated with the NAS architecture capabilities. Critical failures are divided into two categories: those that pose a significant safety risk, and those that only affect system capacity. There is no STLSC corresponding to “routine” because a top-down allocation of availability would result in unacceptably low RMA requirements that could lead to unreliable systems with excessive maintenance costs.

Acquisition Managers need only to identify the service thread(s) associated with the system being acquired, identify the service thread with the highest service thread loss criticality, and apply the RMA requirements associated with that category to the system.

Most system acquisitions can be accommodated within the existing service thread structure, as they are replacing or improving components within an existing service thread. However, when systems providing an entirely new service are planned, it will be necessary to coordinate with System Engineering in defining new service threads.

In addition to the quantitative RMA requirements, the following RMA related characteristics need to be addressed:

- **Scheduled Downtime** – Although scheduled downtime is beyond the contractor’s ability to control, it is still an important factor in ensuring the operational suitability of the system being acquired, and the need to accommodate scheduled downtime without operational disruption is a necessary factor in acquisition planning.

  Many systems are not needed on a 24/7 basis; some airports restrict late operations, and some weather systems are only needed during periods of adverse weather. If projected downtime requirements can be accommodated without unduly disrupting Air Traffic Control operations by scheduling downtime during low traffic periods or when the system is not needed, then there is no impact.

  Conversely, if scheduled downtime cannot be accommodated without disrupting air traffic control operations, it is necessary to re-examine the approach being considered. It also may be necessary to add an independent backup system to supply the needed service while the primary system is unavailable.

- **Redundancy and Fault Tolerance Requirements** – The first determinant of the need for redundancy and fault tolerance is the required inherent availability of the hardware architecture. If the failure and repair rates of a single set of system elements cannot support the inherent availability requirements, redundancy and automatic fault detection

and recovery mechanisms must be added. There must be an adequate number of hardware elements that, given their failure and repair rates, the combinatorial probability of running out of spares is consistent with the inherent availability requirements. When it is determined that redundancy and fault tolerance are required to meet RMA requirements, the performance characteristics of the fault tolerance mechanisms such as switchover times and restart times need to be specified.

There are other reasons beyond the inherent availability of the hardware architecture that may dictate a need for redundancy and/or fault tolerance. Even if the system hardware can meet the inherent hardware availability, redundancy may be required to achieve the required recovery times and provide the capability to recover from software failures.

All Service Threads with a STLSC of “Efficiency-Critical” have rapid recovery time requirements because of the potentially severe consequences of lengthy service interruptions on the efficiency of NAS operations. These recovery time requirements will, in all probability, call for the use of redundancy and fault-tolerant techniques. The lengthy times associated with rebooting a computer to recover from software failures or “hangs” indicates a need for a standby computer that can rapidly take over from a failed computer.

For a complete discussion of the allocation process and preliminary requirements analysis, see Sections 6 and 7.1 of the RMA Handbook.

Task 2: Procurement package preparation

The primary objectives to be achieved in preparing the procurement package are as follows:

- To provide the specifications that define the RMA and fault tolerance requirements for the delivered system and form the basis of a binding contract between the successful offeror and the Government.
- To define the effort required of the contractor to provide the documentation, engineering, and testing needed to monitor the design and development effort, and to support risk management, design validation, and reliability growth testing activities.
- To provide guidance to prospective offerors concerning the content of the RMA sections of the technical proposal, including design descriptions and program management data required to facilitate the technical evaluation of the offeror’s fault-tolerant design approach, risk management, software fault avoidance and reliability growth programs.

The RMA-related parts of the procurement package include:

- **System-Level Specification (SLS)** – The System-Level Specification serves as the contractual basis for defining the design characteristics and performance that are expected of the system. From the standpoint of fault tolerance and RMA characteristics, it is necessary to define the quantitative RMA and performance characteristics of the automatic fault detection and recovery mechanisms. It is also necessary to define the operational requirements needed to permit FAA facilities personnel to perform real-time monitoring and control and manual recovery operations as well as diagnostic and support activities. In addition, the SLS RMA requirements should include parameters that specify the reliability growth required from the first system deployment to the last system deployment.
- **Statement of Work (SOW)** – The Statement of Work describes the RMA-related tasks required of the contractor to design, analyze, and monitor risk; implement fault avoidance programs; and prepare the documentation and engineering support required to provide Government oversight of the RMA, Monitor and Control function, fault-tolerant design effort, support fault-tolerance risk management, and conduct reliability growth testing.
- **Information for Proposal Preparation (IFPP)** – The IFPP describes material that the Government expects to be included in the offeror’s proposal.

Preparation of the RMA procurement package components is discussed in Section 7.2 of the RMA Handbook.

Task 3: Proposal evaluation

The following topics represent the key factors in evaluating each offeror's approach to developing a system that will meet the operational needs for reliability and availability:

- **Reliability Modeling and Assessment** – The evaluation of the offeror's inherent availability model is simple and straightforward. All that is required is to confirm that the model accurately represents the architecture and that the mathematical formulas are correct. The substantiation of the offeror's MTBF and MTTR values used as inputs to the model should be also reviewed and evaluated. Appendix B of the RMA Handbook provides tables and charts that can be used to check each offeror's RMA model.
- **Fault-Tolerant Design Evaluation** – The offeror's proposed design for automatic fault detection and recovery/redundancy management should be evaluated for its completeness and consistency. A critical factor in the evaluation is the substantiation of the design's compliance with the recovery time requirements. There are two key aspects of the fault-tolerant design. The first is the design of the software components that contain the protocols for health monitoring, fault detection, error recovery, and redundancy management. Equally important is the offeror's strategy for incorporating fault tolerance into the application software. Unless fault tolerance is embedded into the application software, the ability of the automatic recovery software to effectively mask software faults will be severely limited. The ability to handle unwanted, unanticipated, or erroneous inputs and responses must be incorporated during the development of the application software.
- **Performance Modeling and Assessment** – An offeror should present a complete model of the predicted system loads, capacity, and response times. Government experts in performance modeling should evaluate these models. Fault tolerance evaluators should review the models in the following areas:
  - **Latency of fault tolerance protocols** – The ability to respond within the allocated response time is critical to the success of the fault tolerance design. It should be noted that, at the proposal stage, the level of the design may not be adequate to address this issue.
  - **System Monitoring Overhead and Response Times** – The offeror should provide predictions of the additional processor loading generated to support both the system monitoring performed by the M&C function as well as by the fault tolerance heartbeat protocols and error reporting functions. Both steady-state loads and peak loads generated during fault conditions should be considered.
  - **Relation to Overall System Capacity and Response Times** – The system should be sized with sufficient reserve capacity to accommodate peaks in the external workload without causing slowdowns in the processing of fault tolerance protocols. Adequate memory should be provided to avoid paging delays that are not included in the model predictions.

Fault Tree Analysis

Fault Tree Analysis (FTA) is a popular and productive risk identification tool. It provides a standardized discipline to evaluate and control hazards. The FTA process is used to solve a wide variety of problems ranging from safety to management issues.

This tool is used by engineers both prevent and resolve hazards, failures and risks. Both qualitative and quantitative methods are used to identify areas in a system that is most critical to safe operation. Either approach is effective. The output is a graphical presentation providing technical and administrative personnel with a map of "failure or hazard" paths.

The FTA is a graphical logic representation of fault events that may occur to a functional system. This logical analysis must be a functional representation of the system and must include all combinations of system fault events that can cause or contribute to the undesired event. Each contributing fault event should be further analyzed to determine the logical relationships of underlying fault events that may cause them. This tree of fault events is expanded until all "input" fault events are defined in terms of basic, identifiable faults that may then be quantified for computation of probabilities, if desired. When the tree has been completed, it becomes a logic

gate network of fault paths, both singular and multiple, containing combinations of events and conditions that include primary, secondary, and upstream inputs that may influence or command the hazardous mode.

Based on available data, probabilities of occurrences for each event can be assigned. Algebraic expressions can be formulated to determine the probability of the top level event occurring. This can be compared to acceptable thresholds and the necessity and direction of corrective action determined. The FTA shows the logical connections between failure events and the top level hazard or event. "Event," the terminology used, is an occurrence of any kind. Hazards and normal or abnormal system operations are examples.

The FTA's graphical format is superior to the tabular or matrix format in that the inter-relationships are obvious. The FTA graphic format is a good tool for the analyst not knowledgeable of the system being examined. The matrix format is still necessary for a hazard analysis to pick up severity, criticality, family tree, probability of event, cause of event, and other information. Being a top-down approach, in contrast to the fault hazard and FMECA (see below), the FTA may miss some non-obvious top-level hazards.

Failure Modes and Effects Analysis (FMEA) and Failure Modes and Effects Criticality Analysis (FMECA)

The scope of this effort depends on system complexity, subsystem and external interfaces, and new design elements. The effort also impacts maintainability, testability, logistics, and safety analyses.

FMEA is an evaluation process for analyzing and assessing the potential failures in a system. The objective is to determine the effect of failures on system operation, identify the failures critical to operational success and personnel safety, and assess each potential failure according to the effects on other portions of the system. In general, these objectives are accomplished by itemizing and evaluating system composition and functions.

FMEA is a systematic method of identifying the failure modes of a system, a constituent piece, or function and determining the effects on the next higher level of the design. The detection method (if any) for each failure mode may also be determined. An FMEA may be a quantitative or qualitative analysis and may be performed on all types of systems (e.g., electrical, electronic, or mechanical). If a quantitative FMEA is being performed, a failure rate is determined for each failure mode. The FMEA results may be used to support other analysis techniques, such as a fault tree analysis. Other techniques that are occasionally used include the dependence diagram and Markov analysis.

Adding a criticality figure of merit is needed to generate the FMECA from the FMEA. Assigning severity levels cannot be performed without first identifying the purpose of the FMECA.

See Section 7.3 of the RMA Handbook for a more detailed discussion of these topics.

Task 4: Contractor design monitoring

The following activities should be conducted by FAA specialty engineers during system development:

- **Formal Design Reviews** – Formal design reviews are a contractual requirement. Although these reviews are often too large and formal to include a meaningful dialog with the contractor, they do present an opportunity to escalate technical issues to management’s attention.
- **Technical Interchange Meetings (TIM)** – The contractor’s design progress should be reviewed in a monthly Fault Tolerance TIM. In addition to describing the design, the TIM should address the key timing parameters governing the operation of the fault tolerance protocols, the values allocated to the parameters, and the results of model predictions and or measurements made to substantiate the allocations.
- **Fault Tolerance Design Risk Management** – The objective of the fault tolerance risk management activities is to expose flaws in the design as early as possible, so that they can be corrected “off the critical path” without affecting the overall program cost and schedule. Typically, major acquisition programs place major emphasis on formal design

reviews such as the System Requirements Review (SRR), the System Design Review (SDR) the Preliminary Design Review (PDR), and the Critical Design Review (CDR). After the CDR has been successfully completed, lists of Computer Program Configuration Items (CPCIs) are released for coding, beginning the implementation phase of the contract. After CDR, there are no additional formal technical software reviews until the end of implementation phase when the Functional and Physical Configuration Audits (FCA and PCA) and formal acceptance tests are conducted. Separate fault tolerance risk management activities should be established for:

- Fault-tolerant infrastructure
- Error handling in software applications
- Performance monitoring

The fault tolerance mechanisms will generally be developed by individuals whose primary objective is to deliver a working fault detection and recovery capability. Risk management activities associated with the fault tolerance mechanism development are directed toward uncovering logic flaws and timing/performance problems.

In contrast, application developers are *not* primarily concerned with fault tolerance. Their main challenge is to develop the functionality required of the application. Under schedule pressure to demonstrate the required functionality, building in the fault tolerance capabilities that need to be embedded into the application software is often overlooked or indefinitely postponed during the development of the application. Once the development has been largely completed, it can be extremely difficult to incorporate fault tolerance into the applications after the fact. Risk management for software application fault tolerance consists of establishing standards for applications developers and ensuring that the standards are followed.

Risk management of performance is typically focused on the operational functionality of the system. Special emphasis needs to be placed on the performance monitoring risk management activity to make sure that failure detection, failure recovery operations, system initialization/re-initialization, and switchover characteristics are properly modeled.

See Section 7.4 of the RMA Handbook for a more detailed discussion of these topics.

Task 5: Design validation and reliability growth

As discussed previously, it is not possible to verify compliance with stringent reliability requirements within practical cost and schedule constraints. There is, however, much that can be done to build confidence in the design and operation of the fault tolerance mechanisms and in the overall stability of the system and its readiness for deployment.

Fault Tolerance Diagnostic Testing – Despite an aggressive risk management program, many performance and stability problems do not materialize until large scale testing begins. The System Analysis Recording (SAR) and the Data Reduction and Analysis (DR&A) capabilities provide an opportunity to leverage the data recorded during system testing to observe the operation of the fault tolerance protocols and diagnose problems and abnormalities experienced during their operation.

For system testing to be effective, the SAR and DR&A capabilities should be available when testing begins. Without these capabilities, it is difficult to diagnose and correct internal software problems.

Functional Testing – Much of the test time at the FAA William J. Hughes Technical Center (WJHTC) is devoted to verifying compliance with each of the functional requirements. This testing should also include verification of compliance with the functional requirements for the systems operations functions including:

- Monitor and Control (M&C)
- System Analysis Recording (SAR)
- Data Reduction and Analysis (DR&A)

Reliability Growth Testing – A formal reliability demonstration test in which the system is either accepted or rejected based on the test results is not feasible. The test time required to obtain a statistically valid sample is prohibitive, and the large number of software failures encountered in any major software development program would virtually ensure failure to demonstrate compliance with the requirements. Establishing "pass-fail" criteria for a major system acquisition is not a viable alternative.

Reliability growth testing is an on-going process of testing and correcting failures. Reliability growth was initially developed to discover and correct hardware design defects. Statistical methods were developed to predict the system MTBF at any point in time and to estimate the additional test time required to achieve a given MTBF goal.

Reliability growth testing applied to automation systems is primarily a process of exposing and correcting latent software defects. The hundreds of software defects exposed during system testing, coupled with the stringent reliability requirements for these systems, preclude the use of statistical methods to accurately predict the test time to reach a given MTBF prior to system deployment. There is no statistically valid way to verify compliance with reliability requirements at the WJHTC prior to field deployment. There is a simple reason for this: it is not possible to obtain enough operating hours at the WJHTC to reduce the number of latent defects to the level needed to meet the reliability requirements.

The inescapable conclusion is that it will be necessary to field systems that fall short of meeting the reliability requirements. The large number of additional operating hours accumulated by multiple system installations will increase the rate that software errors are found and corrected and the growth of the system MTBF.

To be successful, the reliability growth program must address two issues. First, the contractor must be aggressive at promptly correcting software defects. The contractor must be given a powerful incentive to keep the best people on the job through its completion, instead of moving them to work on new opportunities. The first step is to establish initial and final reliability targets from the outset in the System Level Specification. The second step is accomplished during the testing phase by a process called "expunging." The system MTBF is computed by dividing the operating hours by the number of failures. However if the contractor demonstrates that the cause of a failure has been corrected, then the failure is "expunged" from the list of failures. If a failure cannot be repeated within 30 days, it is also expunged from the database.

Thus, if all Program Trouble Reports (PTR) are fixed immediately, the computed MTBF would be infinite even if the system were continuing to fail on daily basis. This measure is statistically meaningless as an indicator of the system's true MTBF. It is, however, a useful metric for assessing the responsiveness of the contractor in fixing the backlog of accumulated PTRs. Since the Government representatives decide when to expunge failures from the database, they have considerable leverage over the contractor by controlling the value of the MTBF reported to senior program management officials. There may be other or better metrics that could be used to measure the contractor's responsiveness in fixing PTRs. The important thing is that there must be a process in place to measure the success of the contractor's support of reliability growth.

A second issue that must be addressed during the reliability growth program is the acceptability of the system to field personnel. In all probability, the system will be deployed to field sites before it has met the reliability requirements. Government field personnel should be involved in the reliability growth testing at the WJHTC and concur in the decision concerning when the system is sufficiently stable to warrant sending it to the field.

See Section 7.5 of the RMA Handbook for a more detailed discussion of these topics.

Task 6: RMA requirements analysis and maintenance

NAS-RD Maintenance – Clearly, if the NAS-RD is to be effective in guiding the evolution of the NAS Architecture, it has to be a living document. The RMA requirements have been designed so that, with the exception of the Service Threads, they should be largely independent of changes in the NAS Architecture or the NAS-RD functional requirements. The basic concept of assigning a STLSC to a Service Thread and applying the RMA requirements associated with the STLSC to the Service Thread is independent of the evolution of the NAS architecture.

One of the advantages of the Service Thread based approach is that the Service Threads will remain relatively constant as the NAS Architecture evolves. Many, if not most, of the changes to the NAS Architecture involve replacement of a subsystem represented by a single block in the reliability block diagram for a Service Thread. Thus, the basic thread does not need to change, only the name of a block in the thread. As the NAS evolves, the Service Thread Diagrams should evolve with it.

While the addition of a new Service Thread to the NAS should be a relatively rare occurrence, Service Threads may need to be added in the future to accommodate new NAS capabilities. Provisions should be made so that it is not overly difficult to make these additions. Maintaining a flexible approach to Service Thread mapping will facilitate the accommodation of new threads when they are needed.

RMA Requirements Assessment – The NAS-RD RMA requirements have been rewritten to allocate RMA requirements to Service Threads that are based on the National Airspace Performance Reporting System (NAPRS) services defined in FAA Order 6040.15. The Service Thread approach applies the NAS-Level requirements to real-world services and facilities that are precisely defined and well-understood in both the engineering *and* operational communities in the FAA.

Several benefits accrue from using this approach, including the ability to “close the loop” between the measured RMA characteristics of operational services and systems and the NAS-Level requirements for these systems. Previously, the only real feedback reconciling RMA requirements with the actual performance of systems has been part of the WJHTC testing of newly developed systems. Linking the NAS-level requirements to NAPRS operational services allows system engineers to assess the reasonableness of the requirements by comparing them with the achieved reliability and availability of currently deployed systems.

This topic is discussed in more detail in Sections 8 and 9 of the RMA Handbook.

5.1.5 Outputs

- **Preliminary Requirements Analysis** – The preliminary RMA requirements analysis has been completed and documented in NAS-RD and the RMA Handbook.
- **Procurement Package Development** – The following RMA engineering outputs are needed by acquisition managers responsible for preparing the procurement package:
  - RMA- and fault-tolerance-related sections of the System Level Specification
  - RMA- and fault-tolerance-related sections of the Statement of Work (SOW)
  - Data Item Descriptions for RMA- and fault-tolerance-related deliverables
  - RMA and fault tolerance items to be included in the IFPP
- Proposal Evaluation
  - RMA Model Assessment
  - Fault Tolerance Design Evaluation
  - Fault Tolerance Performance Assessment
- Contractor Design Monitoring
  - Formal Design Reviews
  - Technical Interchange Meetings
  - Fault Tolerance Design Risk Management
- Testing and Verification
  - Fault Tolerance Diagnostic Testing
  - Functional Testing
  - Reliability Growth Testing

- Requirements Analysis and Maintenance
  - NAS-RD Maintenance
  - Requirements Analysis

Additional Information

For sources of information used to generate content throughout this section, see References.

5.2 Life Cycle Engineering

Life Cycle Engineering (LCE) is defined as an objective process to evaluate the constraints and dependencies associated with developing and operating a product or service over its entire useful life. Life Cycle Engineering seeks to maximize a product's value while minimizing its cost of ownership over its lifetime. The lifecycle includes the entire spectrum of activity for a given system, starting with identification of a need and extending through design and development, production and construction, operational use, sustainment of support and system retirement, and, eventually, disposal.

LCE design considerations address procurement and other issues related to the entire product useful life. It must account for the environment in which the product will operate, as this can affect the product's cost and duration. Decisions made in early phases of the lifecycle affect the overall cost throughout the lifecycle. Procurement costs are the most apparent costs associated with the early lifecycle. Costs that occur later in the lifecycle, such as maintenance costs, are directly related to decisions made in planning and procurement activity. Consequently, LCE focuses on design, implementation, and operational decisions that will significantly impact the product lifecycle cost.

LCE work supports identification of cost/benefit tradeoffs, determines design progress, measures technical soundness, and supports mitigation of risk items. The main objective of LCE is to meet the cost and performance objectives during the entire product lifecycle. LCE manages costs from inception to disposal – or, cradle to grave – for equipment and projects over their anticipated useful lifespan. LCE aims at providing an engineering discipline that provides best results when both art and science are merged with good judgment.

5.2.1 Life Cycle Engineering Steps

The LCE process consists of the six steps shown in Figure 55. Inputs from other Systems Engineering processes are required to perform LCE, and LCE products are required to effectively support other processes.

LCE activities support the FAA Acquisition Management System (AMS) Lifecycle phases and major decision points. LCE process steps map to these phases. Those same steps identify functional benefits and estimate costs for system features and updates throughout the entire lifecycle. LCE uses Earned Value Measurement (EVM) techniques to define cost and schedule targets and provide the metrics for reporting F&E-funded LCE activity status during the Investment Analysis (IA) and Solution Implementation phases.

As IA proceeds for a proposed system procurement, a Basis of Estimate (BOE) document is typically developed to document the underlying cost assumptions and algorithms into a baseline. The estimate must be updated continuously over the program's life to account for cost, schedule, and technical changes and it provides an input to the yearly Resource Planning Document (RPD) submissions. The resulting reports reflect the scope, complexity, and cost performance objectives that the planning activities provide.

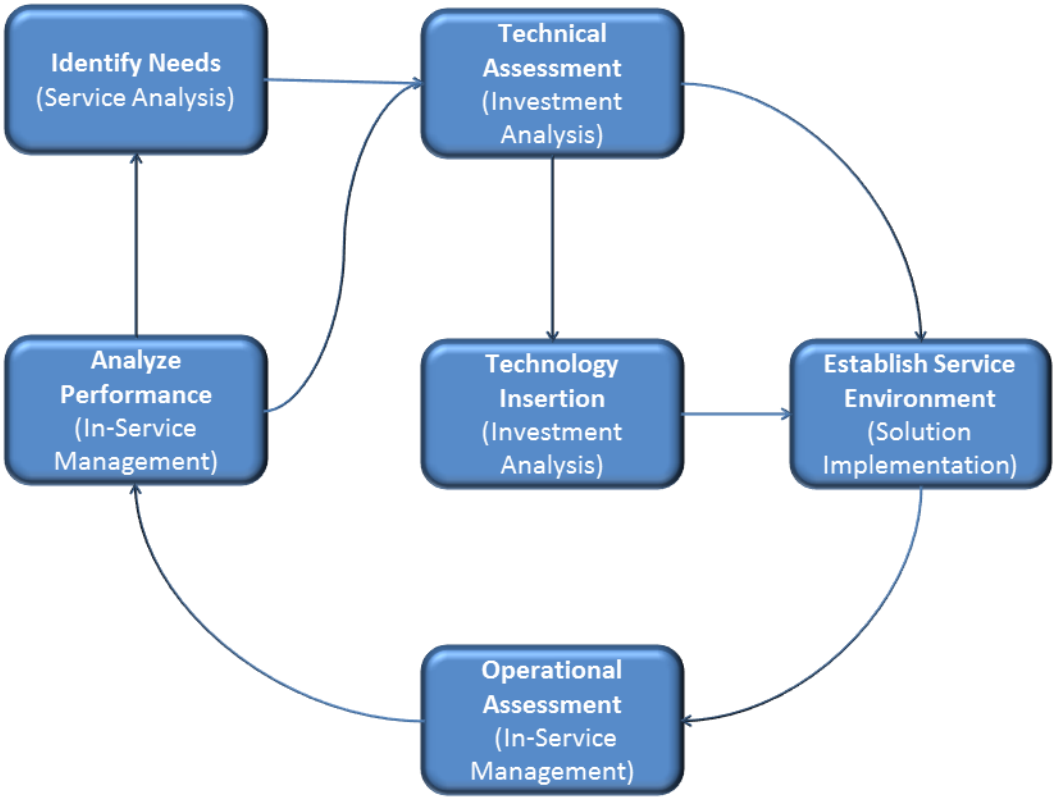


Figure 55: LCE Process Steps

The RPD is used not only to describe how and when F&E development dollars are being planned and expended, but also reflects the In-Service Operations funding for system lifecycle sustainment.

Step 1: Identify needs

LCE identifies system lifecycle requirements, including real estate management, deployment, and transition; integrated logistics support; sustainment; and disposal. Needs are identified primarily during the Service Analysis phase of the system lifecycle.

Identify LCE Support Needs

LCE depends on defined service levels that detail the support needed from other systems and services. These needs, and those of the program, determine the means for delivering projected services. This step identifies the demand for services, as defined in the Service Gap Analysis during the AMS Service Analysis phase. Often, a system's mission is to extend the capabilities of other services (*e.g.*, system capabilities to meet additional performance requirements). The services being "extended" in this manner are a key element in determining the performance of the system under question. Changes to the original system will affect the services provided to the system under question, and these changes must be accounted for in the determining the LCE support needs.

For example, the Wide Area Augmentation System is used to augment the integrity of the Department of Defense's NAVSTAR Global Positioning System to meet the needs of civil aviation.

The system's program documentation describes the services that support logistical activities and maintenance support capabilities. An example of such a support service definition is the "supply chain" for supplying material to operations. This material is used to deploy new components for sustaining and expanding the system and also for maintaining and repairing in-service components.

Define Logistics Requirements

LCE defines the logistics requirements for supporting the system resources. Typically, resource support is defined in the context of the system's overall scope and complexity during the entire system lifecycle.

Identify Deployment Needs

Deployment of a system will often be through phases driven by a number of factors, including budget constraints, vendor schedules, technology maturity, service environment, physical infrastructure, and logistics issues. LCE addresses phased deployment and identifies the key events initiating the activities associated with each phase. LCE allocates lifecycle costs to each deployment phase, including costs associated with in-service testing, logistics, and maintenance support.

Define Performance Audit Measurements

LCE identifies and specifies operations and maintenance metrics used to evaluate support performance for systems having multiple deployment phases. Support performance requirements are applied to engineering support functions, maintenance personnel, and supply chain components. Technical performance requirements are established as a result of other SE processes (notably Operational Concepts Development (Section 3.1), Functional Analysis (Section 3.2), Interface Management (Section 4.2), Verification and Validation (Section 4.7)).

Develop Logistics Support Metrics

Discrete lifecycle activities should be consistent with WBS entries and defined in terms of their entry and exit criteria; schedule and cost criteria are then developed to support these criteria. Avoid level-of-effort approximations, except where existing contracts require it.

Step 2: Technical assessment

Technical assessment is evaluated at the In-Service Performance Review (ISPR), which is typically held every two years, after commissioning. The ISPR is a formal, technical review to characterize the In-Service technical and operational health of the deployed system by assessing risk, readiness, technical status, and trends in a measurable form that will substantiate In-Service support and budget priorities. (See Section 4.1: Integrated Technical Management for additional information.)

This assessment addresses not only potential incorporation of existing technology into design solutions, but also looks at the risks and limits imposed by and on that technology. Each alternative considered is analyzed against the changing technologies available in the marketplace. Available technologies are studied for cost-effectiveness, maturity, for use in the design under consideration, for potential improvements to design performance, and for improvement to maintainability of the resulting system.

The technical assessment may indicate that the system is operating sufficiently (within operational and performance criteria), or it may indicate the need to insert new technology to return the system to operational performance criteria. This assessment also provides input into the Operational Analysis process and ultimately into the mandated OMB-300 reports.

Evaluate Performance Audit

Analyze performance audit results and provide concerns and issues to the Risk Management element.

Evaluate Maintenance Support Facility

Evaluate the Maintenance Support Facility capabilities in supporting system maintenance. The results of this evaluation will include lifecycle cost estimates (provided to Requirements Management), and concerns and issues (provided to Risk Management) as work products. This evaluation is especially important as second-level engineering and maintenance support can be over 70% of the program's operations budget.

Step 3: Technology insertion

The need for a new technology that makes a previously unavailable performance or functional improvement a viable option must be carefully weighed against the risk imposed by that technology. The potential benefits of inserting the technology must outweigh the potential risks to cost, schedule, and performance. When considering the potential technology insertion, one must consider the impacts to the end user through human factors analysis (see Section 5.4: Human Factors Engineering).

If the technology assessment indicates new technology is warranted, promising candidate technologies will be evaluated as possible solutions. Some technological opportunities may result, based on the decisions related to the logistics elements. If the decision is to use COTS products, LCE should identify those items that will probably become obsolete. This creates a need to develop a plan to support all COTS items in the out years of the system's lifecycle. The FAA COTS Risk Mitigation Guide provides information and guidance on COTS product obsolescence stages and how to limit their potential effects on system performance.

LCE recommends preplanned product improvement or alternative improvement options. Inputs may include results of an analysis of the existing system showing opportunities for insertion of technology, the technology assessment, a market survey to identify new COTS products available in the commercial marketplace, operations and maintenance costs of existing systems, and results of an Investment Analysis.

LCE may conclude that a technological opportunity is beyond the scope of an existing Acquisition Program Baseline. If technology insertion offers a potential for improving safety, significantly lowering costs, or improving effectiveness, then revise the Service Gap Analysis. The updated Needed Capability section should describe the technological opportunity. The description should not seek to justify a specific solution or an acquisition program.

Technology Insertion (TI) is also considered the step that defines how systems may replace obsolete components and remain in service. This is a result of system activity that identifies components needing replacement due to lack of support or to achieve technical advantage.

TI includes the following steps:

- Identify technological opportunities during the Service Analysis Lifecycle phase
- Collect the technical data to support schedule and cost decisions to make the baseline changes
- Define the support equipment to deploy the proposed system changes
- Identify new technology insertion resulting in changes to the maintenance support facility (*e.g.*, second-level engineering support, outsourcing strategies, and other maintenance requirements).

Step 4: Analyze performance

This LCE step periodically measures the system's performance against the approved baseline (established at the beginning of the LCE steps). The performance criteria are defined in the design and system performance is evaluated periodically throughout the system's lifecycle.

Define Performance Audit Objectives

Performance audits measure the technical performance of a system (or service). They measure each service function provided by the system under consideration for consistency with the service level included with the approved baseline. Since the approved baseline is subject to change over a system's lifecycle, a performance audit will verify the service functions for each service level.

Analyze Investment Performance

There are two stages in investment performance analysis. The first is the AMS Initial Investment Analysis phase, which focuses on the set of viable alternatives. LCE provides a lifecycle cost estimate for each of these alternatives. An important artifact produced at this time is the preliminary program requirements (pPR). The Final Investment Analysis phase refines the physical architecture for the selected alternative and adds maturity to the documentation. The final program requirements (fPR) and the program specification are completed and finalized. LCE provides a refined lifecycle cost based on the fPR.

Steps in the investment performance analysis include the following:

- Identify metrics affected by planned investment objectives. These objectives should support the business by identifying cost, schedule, and technical performance as deviations against the baseline plan.
- Determine lifecycle cost based on primary logistical elements, including costs associated with maintaining computer resources support, support equipment (test equipment and tools), and the maintenance support facility overall system lifecycle phases.

Step 5: Operational assessment

At deployment, the system closely matches the baseline fPR. Over time, either the operational needs can change, or the system can deviate from the baseline due to the service environment, either of which requires an operational assessment.

The Operational Environment Assessment (OEA) is the key measurement of the operational environment's capability to support the system as it is currently configured, according to the approved baseline. The areas considered in this assessment are also described in the National Airspace Integrated Logistics Support (NAILS) documentation. However, the LCE OEA activity is oriented toward monitoring operational processes and support facilities to achieve the values of the deployed system.

Note: Integrated Logistics Support (ILS) and NAILS are the same and are used interchangeably. FAA documentation refers to both NAILS and ILS. Both are included in this explanation in case one or the other term is used during the course of procurement.

Operational performance is monitored and analyzed, and data is provided as a basis for optimizing current operations and planning for future upgrades. The FAA COTS Risk Mitigation Guide/Practical Methods for Effective Acquisition and Support provides information and guidance on COTS product obsolescence stages and how to limit their potential effects on system sustainment.

LCE, in its data analysis, performs the following functions:

- Monitors and analyzes system performance
- Optimizes current operations
- Identifies technology opportunities and plans for future upgrades
- Identifies obsolescence issues and determines the impact

Step 6: Establish service environment

LCE provides the initial scope and complexity assessment for the system or its Service Environment and for any proposed changes. It also manages the system's lifecycle, including real estate management, deployment and transition, integrated logistics support, sustainment, and disposal. It identifies constraints for system lifecycle attributes, including:

- Integrated Logistics Support
- Deployment and Transition
- Real Property Management
- Sustainment
- Disposal

5.2.2 Integrated Logistics Support

Integrated Logistics Support, a critical, functional discipline, establishes and maintains a support system for all FAA products and services. The objective is to provide the required level of service to the end user at minimal lifecycle cost to the agency. This policy applies not only to new acquisition programs, but also to sustainment of fielded products and services. LCE is responsible for all logistics activities during the life of the system and determines all program logistic attributes.

ILS provides a structured discipline for defining support constraints and acquiring support assets so that fielded products can be operated, supported, and maintained effectively over their entire service life. The primary goal of ILS is to provide high product availability at the lowest cost.

ILS is responsible for identification and acquisition of the support items identified as a result of an analysis of the elements. The nine elements FAA uses that need to be addressed are:

- Maintenance planning
- Maintenance support facility
- Direct-work maintenance staffing
- Supply support
- Support equipment
- Training, training support, and personnel skills
- Technical data
- Packaging, handling, storage, and transportation
- Computer resources support

It is fundamental to sound ILS planning that these elements are addressed within the context of each phase of the product's lifecycle (Service Analysis, Investment Analysis, Solution Implementation, and In-Service Management). It is also necessary to manage the interdependencies among these elements within each phase while adhering to the principles of asset supply chain management (*i.e.*, integration of suppliers, users, and schedules).

ILS determines the parameters of the equipment (reliability, maintainability, and availability). These values will have a direct impact on sparing, depot maintenance, training, maintenance planning, and other elements. The key to a successful acquisition is good communication between the logistics representative and the systems engineer.

ILS Inputs

Several inputs are needed to facilitate effective ILS planning and execution. FAA and Air Traffic Organization (ATO) policy, market research, technology, contractor analysis, and other concerns and issues must be considered.

Additionally, design constraints and trade study reports provide information needed to choose between various alternatives.

ILS Process

The typical steps involved in the ILS process are:

- Develop ILS constraints
- Define maintenance concept and support strategy for candidate solution
- Develop ILS performance, cost, and schedule benefits
- Define strategy for satisfying support requirements
- Define work tasks for obtaining support
- Develop ILS input for the procurement package
- Perform support analysis tasks
- Define maintenance support facility constraints
- Acquire ILS assets
- Conduct In-Service Readiness Review for ILS

ILS Outputs

ILS outputs include the Integrated Logistics Support Planning section of the SEMP or LCP, including maintenance concepts, support requirements, and any related concerns and issues. This planning section describes how FAA will support each logistics element. This plan is developed early in the lifecycle, coordinated with systems engineering, and is updated as information is further defined. It forms the basis for the contractor's Integrated Support Plan.

5.2.3 Deployment and Transition

Deployment

Deployment planning prepares for and assesses the readiness of a solution to be implemented and is contained in the LCP. Deployment planning is part of a continuous In-Service Review process that begins early in the lifecycle management process, usually during development of requirements in the Concept and Requirements Development portion of the AMS Service Analysis phase. All programs undergo some degree of deployment planning to ensure that key aspects of fielding a new capability are planned and implemented, as well as to ensure that deployment does not create a critical deficiency in other projects.

Transition

Transition involves all work activities for installing the new system at the key site, ensuring all (or most) In-Service Review (ISR) checklist items have been closed, conducting the tests for reaching the In-Service Decision (ISD), and transitioning from the legacy to the new system. It also covers all work activities to install subsequent systems at each operational site and to qualify them for operational service. These activities include the transition planning section of the LCP, which documents how to transition operations and maintenance from the existing system to the new system.

The scope of activities includes preparing the site, installing and testing the equipment, conducting dual operations, familiarizing field personnel with the new equipment, obtaining full operational support, and removing and disposing of replaced assets. Trouble-free deployment and transition requires thorough planning early in the lifecycle and cooperation between the service organization, facility team, system contractor, and regional and site personnel during deployment.

Deployment and Transition Inputs

The implementation schedule identifies when each site will receive the new equipment and dispose of the old. The test schedule is used in developing the overall deployment or implementation schedule. FAA/ATO policy will identify the steps for deployment and commissioning.

Deployment and Transition Process

Deployment planning involves coordination among and participation by many critical functional disciplines. Tradeoffs among cost, schedule, performance, and benefits relative to these functional disciplines must also include the impact of deployment and implementation considerations. Deployment planning tools (such as a tailored In-Service Review Checklist) assist in identifying, documenting, and resolving deployment and implementation issues. Methods and techniques include, but are not limited to, a tailored application of generic tools; integration of checklist issues with other emerging issues (such as problem test reports from program tests and evaluation); development of action plans to resolve checklists and other items; and documentation of the results of issue resolution and mitigation.

Consistent deployment planning shall be documented in the contractor's Statement of Work and associated efforts. The results of deployment planning (and issue resolution) activities are briefed periodically (*e.g.*, at acquisition reviews), presented at the ISD meeting, summarized in an ISD memorandum, and audited during the post-ISD follow up and monitoring activities. For more detailed guidance, see Section 2.2.5.2: Deployment and Transition.

Deployment and Transition Outputs

Completion of an In-Service Review Checklist and an In-Service Decision allows the system to be deployed to the field, marking the entrance to the Solution Implementation phase of AMS. The

final output of deployment and transition is a commissioned system and the disposal of the old system.

5.2.4 Real Property Management

The Real Property Management process ensures recording of all real property assets that FAA owns, leases, and utilizes. Functions of real property accountability — which are to be documented in an automated information system — include, but are not limited to: documentation, verification, and confirmation of the existence of real property records.

The Assistant Administrator for Financial Services records and manages all FAA real property assets. More information is in FAA's Interim Fixed Asset System database.

Real Property Management Inputs

The inputs include a list of space constraints, location of existing equipment, and recommendations for new or modified facilities for the product. Facility drawings showing equipment location, spares storage, support equipment and test benches, and other items that use space will be identified.

Real Property Management Process

The systems engineer performs the following tasks related to property management:

- Determines whether real estate must be acquired for FAA-related projects by identifying space constraints, locations, and the requirement for new or modified facilities
- Notifies real estate experts of the need for purchase and ensures that the property is recorded in the real estate database upon purchase/lease

Real Property Management Outputs

The results of the real property analysis form the basis to determine what real property is required. Real property management uses this recommendation to obtain any necessary property assets (through purchase, lease, or other arrangement) with assistance of real estate experts.

5.2.5 Sustainment

Sustainment is the activity that ensures that the operational system remains at its required capability and quality.

Sustainment Inputs

The Sustainment/Technology Evolution process may need any or all of the following inputs:

- Design constraints
- External pressures
- Operations and maintenance costs
- A list of spares that are difficult or impossible to obtain
- A list of new technology developments and components that can be used to enhance the sustainment of systems
- A list of new commercial products and results from market research
- Demonstrations by vendors

Sustainment Process

The Service Gap Analysis (SGA) serves as the basis for Investment Analysis and is revalidated at the Investment Decision. LCE shall ensure that logistics inputs are included in this document. As a program proceeds through implementation, fielding, sustainment, upgrade, and eventual replacement, the SGA is revalidated periodically. The service organization, working with the field users, will assess the current performance of existing equipment and provide an analysis of how best to sustain the system, as well as plan for future upgrades or replacements.

The Investment Decision stipulates implementation of any preplanned product improvements. Sustainment resources in the acquisition program baseline are used to upgrade components of fielded products (*e.g.*, printers or processors) as needed. The objective is to develop evolutionary products and rapidly insert new technology rather than to periodically replace fielded products.

LCE assists the service organization and its systems engineering efforts throughout the lifecycle in collecting and assessing data for use in evaluating product or service effectiveness. These activities shall include:

- Tracking and evaluating reliability, maintainability, and availability performance and supportability issues
- Analyzing supportability issues caused by market-driven products and analyzing system or subsystem obsolescence
- Determining the most cost-effective means of avoiding projected supportability shortfalls
- Assessing integration of obsolescence-driven system changes with new constraints
- Evaluating the impact of engineering changes, performance shortfalls, or technological opportunities on ILS products and support services
- Supporting revalidation or development of Preliminary Shortfall Analysis Report

Sustainment Outputs

LCE produces a plan to correct systemic problems, remove defects from systems, and implement planned upgrades. It also produces a list of emerging shortfalls and technology enhancements for future systems. Lessons-learned databases may contain samples of these plans, or the service organization may have examples.

Service Life Extension Programs may be used to keep older systems in the field by incorporating new technology. This may increase the service life of the system and lower maintenance costs.

5.2.6 Disposal

An important element of any product's lifecycle is the process used to remove facilities from the operational inventory and ultimately dispose of them. Besides funding concerns, a number of logistics issues shall be considered as a system approaches the end of its commissioned life.

Disposal includes all activities associated with disposal management; dismantlement / demolition / removal; restoration; degaussing / destruction of storage media; and salvage of decommissioned equipment, systems, or sites.

Disposal Inputs

Potential inputs include:

- The implementation schedule for the new system and proposed dates for removal of the existing system
- A list of spares, line replaceable units, documentation, and other items related to the system being replaced
- A list of any hazardous materials or items that need special handling

Disposal Process

SE efforts to support disposal of a system being replaced occur during the new system's implementation phase. Integrated Technical Management (Section 4.1) is used to develop a Disposal Plan conforming to FAA Order 4800.2, Utilization and Disposal of Excess and Surplus Personal Property. LCE supports the ITP process in developing a disposal plan that identifies the systems, components, assemblies, and so forth that will be removed, disposed of, or cannibalized; any environmental issues; place of disposition; the person responsible for disposal; and many other factors. Previous disposal plans contain examples of items that should be considered.

LCE shall conduct an assessment of the system to determine the need to scavenge usable parts/subsystems from facilities slated to be decommissioned. This source of usable parts/subsystems is particularly important for items that are no longer being manufactured. This opportunity must be weighed against the costs of component removal, shipping, shop/vendor refurbishment, and warehousing. LCE may require the expertise of an engineering service in determining the existence of any hazardous materials within the system.

Disposal Outputs

Outputs may include:

- A schedule identifying when each existing system will be removed and shipped to a disposal location
- A list of items that contain hazardous materials or precious metals or that need special handling
- A list identifying items that can be used in other systems

5.2.7 Tools

LCE tools include:

- **Logistics Information System**. This is the inventory control and ordering system for the FAA.
- **Spares Planning Model**. This model assists in the provisioning process by estimating the range and quantity of spares based on failure rates, cost, and other factors.
- **Logistics Management Information guidance**. This guidance is used to identify to the contractor the logistics analysis required on the system and the expected outcome.
- **Bar coding. T**his methodology is defined in the statement of work. It is used to track spares and configuration management of the system.
- **FAA Acquisition System Toolset (FAST)**. This is FAA's reference for all documents and tools used during the acquisition process.
- **Interim Fixed Asset System database**. A database managed by Financial Services, records real property assets.

Additional Information

For sources of information used to generate content throughout this section, see References.

5.3 Electromagnetic Environmental Effects and Spectrum Management

Electromagnetic Environmental Effects (E^3) and Spectrum Management are two closely related areas of Specialty Engineering. Both are involved in handling how various types of radiation affect systems, and how to mitigate such effects. They differ, however, in several ways, and the following sections discuss each area separately, starting with E^3.

5.3.1 Electromagnetic Environmental Effects

E^3 Engineering is the technical discipline dealing with the safe and efficient operation of electronic devices regarding radiated and conducted electromagnetic emissions. This includes both a given system's ability to deal with such emissions from its operational environment and how the device itself affects that environment. E^3 activities seek to minimize how systems are limited by electromagnetic factors, and to document limitations and vulnerabilities that remain after a system's deployment.

Electromagnetic Environmental Effects Engineering

E^3 Engineering is a set of Specialty Engineering analyses/requirements that relate to electronic systems. Such systems range from electric household appliances to integrated circuits.

The Federal Communications Commission (FCC) develops and enforces government regulations related to E^3 and gives special attention to what it calls "digital devices." The FCC defines a digital device as:

> “An unintentional radiator (device or system) that generates and uses timing signals or pulses at a rate in excess of 9,000 pulses (cycles) per second and uses digital techniques;”

These devices must be designed to conform to government regulations on electromagnetic emissions.

Systems Engineering Role: All systems deployed in FAA must conform to government regulations. E3 analyses will be performed to ensure that all electronic systems function properly within an operational environment and that they are compatible with non-electronic elements of that environment. These analyses will also identify problems that could arise from changes in the environment.

There are many types of E3 that may affect a system’s electromagnetic compatibility. Each type is an individual specialty area. From a broad perspective, the operational requirements are to properly address the electromagnetic environment over the system lifecycle. The following sections discuss the individual elements of E3. (Note: E3-related definitions appear in American National Standards Institute (ANSI) C63.14.)

The Electromagnetic Environment

The Electromagnetic Environment (EME) consists of the systems and other elements (i.e., humans and nature) that exist within the area where a given system is or may be operated. Identifying and describing the EME is a major part of E^3. This involves describing all electromagnetic interference (EMI) within the environment and vulnerabilities to systems and other elements of the environment.

Systems Engineering Role: The systems engineer must develop a complete description of the normal EME within which the system, subsystem, or equipment may be required to perform. In some instances, COTS systems have defined the *survivable* EME for a system; that is, the most extreme conditions (EMI present) within which the system may operate safely and without degrading its function.

Electromagnetic Compatibility

Electromagnetic Compatibility (EMC) is the ability of a system to function within its EME and not be a source of troublesome EMI. EMC analyses involve evaluating the EME (all EMI present within that environment) and the new system's own EMI emissions.

Two general types of emissions are considered in an EMC analysis that evaluates EMI: conducted emissions and radiated emissions. Conducted emissions are electric currents transferred through physical coupling, such as noise fed back into a device's alternating current (AC) power system. Radiated emissions are EM waves emitted intentionally or unintentionally that may be unintentionally received by other systems. Wires transmit and receive EM signals like traditional antennas. Switching waveforms in circuits generates a wide band of EM emissions.

Systems Engineering Role: The systems engineer uses EMC analysis data to determine if either the new system or the elements of the operational environment adversely affect each other. EMC considerations are critically important and must be seen as design objectives beyond those required for the basic functional performance of an electronic system. This ensures that a system that functions properly in the laboratory will not have problems when it is deployed within a different EME. The General Requirements for Electronic Equipment (FAA-G-2100) paragraph 3.3.2 Electromagnetic Compatibility—a requirement for any acquisition, which references all appropriate FCC rules and FAA-referenced Military Standards—ensures consideration of EMC throughout the system lifecycle.

Electromagnetic Susceptibility

EM Susceptibility (EMS) specifically deals with a system's operational failure threshold due to weaknesses or lack of resiliency regarding certain EM conditions. A *susceptibility* is a condition that degrades a system. For example, conducted susceptibility refers to a system's inability to withstand an infusion of noise into its power lines.

A *vulnerable* system is defined as a system with the potential to degrade within certain potential EMEs. Any system may be exposed to different operational EMEs during its lifetime, and vulnerability analysis must be performed to head off potential trouble.

Systems Engineering Role: The systems engineer must ensure that susceptibilities and vulnerabilities are addressed before implementation of a system. For example, devices that run on standard AC power must not be susceptible to sudden brief spikes or losses of power if the power system is affected by lightning or other surges. Similarly, an EMS analysis must be conducted to determine the operational impacts of laboratory-observed susceptibilities and vulnerabilities.

Hazards of Electromagnetic Radiation

Hazards of EM Radiation (RADHAZ) are areas of E^3 that deal with specific types of dangers related to radiated EM waves. The two primary RADHAZ evaluated are Hazards of EM Radiation to Fuels (HERF) and Hazards of EM Radiation to Personnel (HERP). HERF is a RADHAZ area dealing with fuels that may be present within an EME. An EM field of sufficient intensity may create sparks that may ignite volatile combustibles, such as fuel (*i.e.*, EM radiation may induce a current in a conductive material, and form sparks in the air gap between two conductors).

HERP deals with the dangers of EM radiation to humans within the EME. When a person absorbs microwaves, the body heats up. Microwave absorption at high power levels (i.e., from radar towers) is sometimes hazardous. Also, EM waves in the x-ray range and higher (in terms of frequency) may cause ionization, even at low power levels.

Systems Engineering Role: It is difficult to locate all potential antennas and spark gaps within an EME, so systems engineers need to keep the power densities of EM fields within safety margins when fuels are present. The systems engineer must also consider RADHAZ in the E^3 analysis to ensure safety for the non-electronic elements of an EME, such as humans and nature.

Electromagnetic Pulse

An EM Pulse (EMP) is an intense burst of EMI, such as that caused by a nuclear explosion. This pulse may damage sensitive electronic systems or cause them to temporarily malfunction. Evaluating the need to perform an analysis on EMP susceptibility is recommended.

Electrostatic Discharge

An Electrostatic Discharge (ESD) is an unintentional transfer of static electricity from one object to another. Static voltage transferred from a human to a device (e.g., voltage generated by walking across a carpet) may be as high as 25 kilovolts. The brief currents created may damage or cause

malfunction of integrated circuits and other electronics. Evaluating the need to perform an ESD susceptibility analysis is recommended.

Lightning

Lightning gets special attention within E^3 because of its tremendous power levels and multiple effects. Lightning effects are *direct* (physical effects) and *indirect* (induced electrical transients and interaction of the EM fields associated with lightning). Determining a need for analysis for susceptibility to lightning is recommended.

Precipitation Static

Precipitation Static (P-Static) is the buildup of static electricity resulting from an object's exposure to moving air, fluid, or tiny solid particles (e.g., snow or ice). It may cause significant ESD and is a particularly important consideration regarding systems aboard aircraft and spacecraft. Evaluating the need for an analysis on P-Static susceptibility is recommended.

Objective

Beyond their mandatory inclusion through regulations, E^3 activities serve to reduce costs, improve system designs, aid in preventing hazards, and to satisfy international concerns. The benefits and satisfaction of laws make E^3 an indispensable part of any systems engineering endeavor.

Government Regulations

The FCC develops and enforces government regulations relating to E^3. Before a new electronic device may be sold in the United States, it must meet FCC standards. These standards are in Rules and Regulations of Title 47 (Part 15) of the Code of Federal Regulations (CFR).

FCC requirements focus on a system's generated EMI, rather than its EMS. The requirements impose limits on the conducted and radiated emissions of digital devices and strictly regulate radiated emissions in terms of the electric field. Most NAS-related electronic/radio frequency devices fall under FCC Class A (commercial, industrial, or business) regulations, which are less stringent than Class B (household devices). Government regulations change frequently, so the systems engineer must ensure he has the current requirements. Information is available from the FCC web site. The FCC may request a sample device of a new system to test.

System Performance and Cost of Redesign

While manufacturers and developers strive to meet government regulations, they may impose additional E^3 requirements on a new system to enhance product performance and customer satisfaction. Government E^3 requirements do not guarantee a new system's compatibility with its intended operational environment. Thus, it is up to manufacturers and developers to consider the EME for a new system, the impacts of the system's own EMI on that environment, and the system's EMS in order to avoid potential problems that FCC regulations are unable to predict or prevent.

Developers and manufacturers who consider potential E^3 problems from the start may avoid costly redesign later. The earlier in a system's lifecycle that a problem is identified, the less the cost of correcting it is likely to be. For instance, if a problem with EMC is discovered after a new system has been deployed, the system may have to undergo extensive redevelopment. However, if this problem had been determined during the design and planning stage, it could have been addressed in the requirements before manufacture had begun, saving both significant time and resources.

Hazard Prevention

Hazards of EM radiation on fuels (HERF) and personnel (HERP) are obvious considerations. These issues may be included as part of Safety Risk Management activities, and yet are still considered in E^3.

International Considerations

EMI is increasing throughout the world. Systems that may be used outside of the United States, such as avionics, must be able to deal with types and intensities of EMI present in other countries that may be different from conditions in the United States. It is recommended that such systems be designed specifically focusing on minimizing vulnerability to EM radiation.

Also, it is recommended that consideration be given to the possibility of intentional jamming, which creates significant EMI.

Analyses of Electromagnetic Environmental Effects

This section specifically discusses the various E^3-related analyses. Not all E^3 analyses discussed are necessary for a given system; which analyses are worth the time and resources are determined during planning.

It is recommended that E^3 analyses be performed on COTS systems as well as new systems to ensure compatibility with the EME within which these systems or subsystems may be used. The amount of detail involved with E^3 analyses increases with each subsequent phase of the SE lifecycle. Measurement procedures for evaluating a product's emissions during low-level technical analyses must be clearly spelled out. The EME may undergo appreciable changes at any point during a system's lifecycle. Thus, E^3 analyses are redone to ensure continued EMC of *each* system within the EME.

Description of the Operational Electromagnetic Environment

Before any EMC analyses are conducted, the EME within which the new system may perform must be defined. This definition entails detailing all sources of EMI in the operational environment. EME contributors are gauged by the power levels and frequencies of their emissions and their locations (with respect to the new system). In some cases, it may also be necessary to denote inherent susceptibilities associated with other systems within the EME.

An existing OSED document may be useful as a starting point for an EME description. The OSED contains information about the operational environment and the systems/subsystems associated with the new system. However, the OSED may not describe all EME contributors.

Optionally, a description may be developed of the maximum survivable EME conditions in which the system shall be able to function without degradation. This is useful in cases in which a specific, operational EME may not be identified (*e.g.*, the system may have numerous and appreciably different operational EMEs to which it is expected to be exposed).

Electromagnetic Compatibility Analyses

EMC analyses identify compatibility issues relating to radiated and/or conducted emissions. This involves evaluating how the EME and the system affect each other in terms of EMI.

The system's *electrical dimensions* must be calculated before an EMC analysis is conducted. This is done to determine whether or not simple mathematical methods (e.g., Kirchoff's Laws) are sufficiently accurate for an EMC analysis. If the system is *electrically large*, then simple mathematics is insufficient, and Maxwell's Equations shall instead be employed. These are a set of differential equations that describe an electric field as three-dimensional parameters (x, y, z) and time (t).

Federal Communications Commission Regulations

It is convenient to address FCC compliance issues for EM emissions during EMC analyses since both deal with the system's EMI. While actual testing to verify that FCC requirements are met may not occur until a system is built, incorporating these regulations into requirements from the beginning of system development helps to mitigate compliance problems later.

Analyses of Hazards of Electromagnetic Radiation

RADHAZ analyses are conducted only when they have relevance for a particular system and its environment. For example, if there are no fuels present within the operational EME, an HERF analysis is unnecessary. It is recommended that the types of RADHAZ analyses (if any) to be performed be determined from the EME description.

Electromagnetic Susceptibility Analyses

As with RADHAZ, specific susceptibility analyses are conducted only when they have relevance. Each analysis requires time and resources, so it is impractical to invest in an analysis that has no significance for the system and its EME. Susceptibility analyses include:

Conducted Susceptibility (AC power lines)

- ESD Susceptibility
- Lightning Susceptibility
- P-Static Susceptibility
- EMP Survivability

Outputs and Products of Electromagnetic Environmental Effects

E^3 analyses and predictions must be employed during all phases of an electronic system's lifecycle. The following sections link the outputs of E^3 activities to the overall SE process. However, note that all E^3 analyses, like other Specialty Engineering analyses, shall be documented in a Design Analysis Report.

Requirements

Most E^3 activities result in requirements that feed the Requirements Management process (Section 3.3.2). This includes the Shortfall Analysis, Statement of Work, specifications, and all performance-based requirements.

Concerns and Issues

E^3 activities—in addition to identifying necessary requirements—also identify potential problems that may surface later in a system's lifecycle. It is also good practice to document identified system susceptibilities that are not significant enough to require correction. These issues are included with concerns and issues, which feed the Risk Management process (Section **Error! eference source not found.**).

Verification Criteria

Verification criteria must be provided to ensure that stated E^3 performance requirements are met. It is also important to provide detailed information describing how E^3 testing is performed and how test results are to be interpreted. This feeds the Verification and Validation processes (Section 4.7).

Solutions to Problems of Electromagnetic Environmental Effects

EMC and EMS problems may be corrected through a number of means, including shielding, emission suppression components, and/or modification of the operational environment. However, some problems may not be directly correctable, potentially forcing extensive and costly product redesign. This is why it is beneficial to consider E^3 issues early in a system's development.

5.3.2 Spectrum Management

The radio frequency (RF) spectrum is that portion of the EM spectrum used for *intentionally* transmitting and receiving signals. It is a finite set of frequencies that must be divided efficiently between various government and civilian industries. FAA, the Air Force, and the Navy are the top three spectrum users in the Federal Government. FAA's numerous communications, navigation, and surveillance systems heavily depend on the RF spectrum, as evidenced by the agency's more than 50,000 frequency assignments.

Spectrum Management within the FAA ensures that systems that use RF technology are assigned proper frequency bands and do not degrade the performance of other RF systems.

Definition

FAA Order 6050.19 states that "The radio spectrum, especially aeronautical radio spectrum that is reserved for exclusive worldwide use by international civil aviation, is a scarce and limited resource," and that "The FAA, and civil aviation in general, is committed to the use of new spectrum-efficient technologies and procedures to preserve this precious resource."

Spectrum Management includes distributing FAA's share of the RF spectrum among systems, integrating new RF technologies into FAA, monitoring RF activity to ensure that RF systems do not interfere with one another, and investigating external sources of RF Interference (RFI) that may degrade performance of other systems.

Coordination with Technical Operations Services

Technical Operations Services is an FAA line of business within the Air Traffic Organization (ATO) that manages FAA usage of the radio spectrum and resolves RFI issues by maintaining a network of Frequency Management Officers (FMOs). Nationally, FMOs are the aviation community's points of contact for resolving reported cases of RFI. Spectrum engineers assigned to the Regional Frequency Management Offices perform detailed, onsite investigations to quickly resolve RFI cases to keep the systems operating in an interference-free electromagnetic environment. FMOs can also engineer local or "site-specific" radio frequencies for approval by Technical Operations Services.

The ATO's Office of Technical Operations Services, ATC Spectrum Engineering Services (formerly Spectrum Policy and Management - ASR), oversees Spectrum Management within the FAA. All project teams developing systems that require RF usage must coordinate with ATC Spectrum Engineering Services to ensure that all Spectrum Management issues are addressed correctly, including assigning RF bands. Project teams must contact ATC Spectrum Engineering Services early in the development process and request guidance on spectrum issues.

ATC Spectrum Engineering Services manages FAA usage of the radio spectrum and resolves RFI issues by maintaining a network of Frequency Management Officers (FMOs).

Objective

The safe transport of all individual flights between airports is based on radio frequencies being available and interference free so that all of the aviation systems function properly. FAA's Spectrum Engineering Services Office provides these fundamental services by ensuring radio frequency assets are always clear and available, both now and in the future.

Spectrum Management Is Required for All RF Systems

The National Telecommunications and Information Administration (NTIA), part of the Department of Commerce, is responsible for administering that portion of the spectrum allocated to Federal use. It is empowered to authorize Federal agencies, which demonstrate appropriate needs and satisfy specific requirements, to use the spectrum.

Spectrum Engineering Services (ATC) oversees FAA's assigned RF bands. Project teams developing RF systems must collaborate with Spectrum Engineering Services to obtain specific RF band assignments. Spectrum Engineering Services continues Spectrum Management activities throughout a system's lifecycle (e.g., frequency reassignments, RFI investigations).

RF System Performance

Spectrum Management ensures an interference-free environment for RF systems. Without Spectrum Management, RFI would be difficult to control, and the performance of RF systems would be seriously degraded. The limited number of usable existing frequency bands dictates the need to organize, coordinate, and monitor spectrum use.

Activities of Spectrum Management

Spectrum Management activities involve identifying and maintaining an RF system's transmission frequencies.

Initial RF Band Assignments

FAA's Spectrum Engineering Services will assign frequency bands for operational use with new systems. A new RF system cannot be introduced without obtaining frequency assignments.

RFI Detection and Reporting

New systems must be tested to ensure that they do not transmit noise that may interfere with other RF systems. Spectrum Engineering Services can provide specific testing criteria.

Any external (unaccounted for) RFI that impedes a system's performance during operational use should be reported to the appropriate regional Frequency Management Officer for investigation.

RF Band Modifications

At any point during a system's lifecycle, Spectrum Engineering Services may change frequency band assignments for any or all systems. Reassignments may be needed because of integration of new RF systems, changes in customer needs, RF spectrum allotment adjustments made by the U.S. Office of Spectrum Management, or international issues. Band assignment modifications can occur on a local, national, or international level. Project teams and systems engineers must be prepared to make frequency band adjustments as required by Technical Operations Services.

Outputs and Products of Electromagnetic Environmental Effects

The following sections link the outputs of Spectrum Management activities to the overall System Engineering process. All Spectrum Management issues shall be addressed directly with Technical Operations Services, ATC Spectrum Engineering Services.

Planning Criteria and Initial Requirements Document

During the early Service Analysis stage, the RF system team must determine the need for and submit a request for spectrum support to the Spectrum Engineering Services Office. The initial requirements document process is not complete until the Spectrum Planning Subcommittee approves the request. The feedback from Spectrum Engineering Services Office feeds the Integrated Technical Planning process (Section 4.1) and the Requirements Analysis process (Section 4.2).

Requirements and Constraints

Spectrum Engineering Services may impose requirements and/or constraints on an RF system at any stage of its lifecycle. These requirements and constraints feed the Requirements Analysis process (Section 4.2).

Verification Criteria

Spectrum Engineering Services requires validation for any RF system under development that ensures spectrum usage of the system is within the approved bounds. This feeds the Verification and Validation process (Section 4.7).

Additional Information

For sources of information used to generate content throughout this section, see References.

5.4 Human Factors Engineering

Human Factors Engineering (HFE) is a multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to: (1) equipment, systems, software, and facilities; (2) procedures, jobs, organizational design, workspaces, and environments; and (3) training, staffing, and personnel management to produce safe, comfortable, efficient, and effective human performance.

HFE provides the opportunity to: (1) develop or improve all human interfaces with the system; (2) optimize human/product performance during system operation, maintenance, and support; and (3) make economic decisions on personnel resources, skills, training, and costs. HFE activities can be embedded and integrated into the acquisition of systems and equipment in order to lower lifecycle costs, improve human-system performance, and reduce technical risk. Failure to apply the disciplines of HFE has consistently resulted in development of systems that do not satisfy the needs of the workforce and often results in costly delays and extensive rework.

The people who operate and maintain the hardware/software are just as important as the hardware and the software themselves. The individuals and teams who operate or maintain the system have different knowledge, skills, and abilities, and they operate the hardware/software under various operating conditions, organizational structures, procedures, equipment configurations, and work scenarios. The total composite of these elements and the human component determines the performance, safety, and efficiency of the system. To produce an effective HFE program for any acquisition, one must not only define the system hardware, software, facility, and services, but also the users (operators and maintainers), their attributes, and the environment in which the system will be used.

Applied early in the lifecycle acquisition management process, HFE increases the probability of improved performance, safety, and productivity; decreases lifecycle staffing and training costs; and becomes well integrated into the program's strategy, planning, cost and schedule baselines, and technical tradeoffs. Changes in operational, maintenance, or design concepts during the later phases of an acquisition are expensive and entail high-risk program adjustments. Identifying lifecycle costs and human performance components of system operation and maintenance during investment analysis and requirements definition decreases program risks and long-term operational costs. These benefits apply to COTS and non-developmental items (NDI) as well as to developmental programs.

5.4.1 Inputs

User performance requirements and other inputs to the HFE process come from many sources at various phases of the acquisition lifecycle, starting in Service Analysis & Strategic Planning. The FAA Human Factors Acquisition Job Aid guidelines are in the FAA Acquisition System Toolset (FAST) and provide basic information regarding integration of HFE activities into the acquisition management process. Product teams must be familiar with human factors concepts and processes to embed HFE principles into their acquisition programs.

Table 27 identifies and defines many classes of human interfaces that the product team may need to consider as it plans and implements equipment and system acquisition programs. Analysis of these interfaces provides a basis for determining the inputs to the HFE process tasks. These inputs may include new or previously conducted human factors research, studies, and analyses; human factors standards and guidelines; human factors technical methods and techniques; human performance data criteria; or other human-system interaction information.

Table 27: Human Performance Interfaces in Systems Acquisition

Human Interface Class	Performance Dimension	Performance Objective
Functional Role Interfaces: For operations and maintenance — role of the human versus automation; functional requirements and tasks; manning levels; and skills and training	Task performance	Ability to perform tasks within time and accuracy constraints under all operational conditions
Information Interfaces: Information media, electronic or hardcopy; information characteristics; and the information itself	Information handling/processing performance	Ability to identify, obtain, integrate, understand, interpret, apply, and disseminate information
Environmental Interfaces: Physical, psychological, and tactical environments	Performance under environmental stress	Ability to perform under adverse environmental stress, including heat and cold, vibration, clothing, illumination, reduced visibility, weather, constrained time, and psychological stress
Operational Interfaces: Procedures, job aids, embedded or organic training, and online help	Sustained performance	Ability to maintain performance over time, during heavy workload, and under emergency and degraded conditions
Organizational Interfaces: Job design, policies, lines of authority, management structure, organizational infrastructure	Job performance	Ability to perform jobs, tasks, and functions within the management and organizational structure
Cooperation Interfaces: Communications, inter- personal relations, and team performance	Team performance	Ability to collectively achieve mission objectives
Cognitive Interfaces: Cognitive aspects of human-computer interfaces, situation awareness, decision making, information integration, workload and short-term memory	Cognitive performance	Ability to perform cognitive operations such as solving problems, making decisions, integrating information, and maintaining situation awareness
Physical Interfaces: Physical aspects of the system with which the human interacts (*e.g.*, human computer interfaces, controls and displays, workstations, and facilities)	Operations and maintenance performance	Ability to attain access and perform operations and maintenance at workstations and worksites, and in facilities using controls, displays, support equipment, tools, job aids, workstation configuration, and other instruments

Addressing the human performance limitations and capabilities would be a daunting task unless the task was divided into its many components and unless human factors were detailed in some descriptive taxonomy of issues. Thus, the potential human factors risks and inputs may be reflected as elements of the human factors areas of interest listed in

Table 28. This list of human factors areas of interest should be reviewed during the conduct of analysis supporting the development of human factors plans, requirements, designs, and other activities.

Table 28: Human Factors Areas of Interest

	Human Factors Areas of Interest
1	**Allocation of Functional Roles**: Assigning those roles/requirements/tasks for which the human or equipment performs better while enabling the human to maintain awareness of the operational situation.
2	**Anthropometrics and Biomechanics**: Accommodating the physical attributes of its user population (e.g., from the 1st through 99th percentile levels).
3	**Communications and Teamwork**: Applying system design considerations to enhance required user communications and teamwork.
4	**Culture**: Addressing the organizational and sociological environment into which any change, including new technologies and procedures, will be introduced.
5	**Displays and Controls**: Designing and arranging displays and controls to be consistent with the operator's and maintainer's tasks and actions.
6	**Documentation**: Preparing user documentation and technical manuals in a suitable format of information presentation, at the appropriate reading level, and with the required degree of technical sophistication and clarity.
7	**Environment**: Accommodating environmental factors (including extremes) to which the system will be subjected and understanding the associated effects on human-system performance.
8	**Functional Design**: Applying human-centered design for usability and compatibility with operational and maintenance concepts.
9	**HCI (Human-Computer Interaction)**: Employing effective and consistent user dialogues, interfaces, and procedures across system functions.
10	**Human Error**: Examining design and contextual conditions (including supervisory and organizational influences) as causal factors contributing to human error, and considering objectives for error tolerance, error prevention, and error correction/recovery.
11	**Information Presentation**: Enhancing operator and maintainer performance by using effective and consistent labels, symbols, colors, terms, acronyms, abbreviations, formats, and data fields.
12	**Information Requirements**: Ensuring availability and usability of information needed by the operator and maintainer for a specific task when it is needed, and in a form that is directly usable.
13	**I/O Devices:** Selecting input and output (I/O) methods and devices that allow operators or maintainers to perform tasks, especially critical tasks, quickly and accurately.

	Human Factors Areas of Interest
14	**KSA:** Measuring the knowledge, skills, and abilities (KSA) required to perform job-related tasks, and determining appropriate selection requirements for users.
15	**Operational Suitability:** Ensuring that the system appropriately supports the user in performing intended functions while maintaining interoperability and consistency with other system elements or support systems.
16	**Procedures:** Designing operation and maintenance procedures for simplicity, consistency, and ease of use.
17	**Safety and Health:** Preventing/reducing operator and maintainer exposure to safety and health hazards.
18	**Situation Awareness:** Enabling operators or maintainers to perceive and understand elements of the current situation, and project them to future operational situations.
19	**Special Skills and Tools:** Minimizing the need for special or unique operator or maintainer skills, abilities, tools, or characteristics.
20	**Staffing:** Accommodating constraints and efficiencies for staffing levels and organizational structures.
21	**Training:** Applying methods to enhance operator or maintainer acquisition of the knowledge and skills needed to interface with the system, and designing that system so that these skills are easily learned and retained.
22	**Visual/Auditory Alerts:** Designing visual and auditory alerts (including error messages) to invoke the necessary operator and maintainer response.
23	**Workload:** Assessing the net demands or impacts upon the physical, cognitive, and decision-making resources of an operator or maintainer using objective and subjective performance measures.
24	**Work Space:** Designing adequate work space for personnel and their tools or equipment, and providing sufficient space for the movements and actions that personnel perform during operational and maintenance tasks under normal, adverse, and emergency conditions.

5.4.2 Human Factors Engineering Process

The process of integrating HFE into acquisition programs entails numerous technical and management activities. Many of these activities are conducted iteratively through several phases of the acquisition, and often in a nonlinear sequence. Other subordinate activities including critical task analysis, target audience analysis, cognitive analysis, human-in-the-loop simulation, training needs analysis, and prototyping are also required. A description of these subordinate tasks is in the FAA Human Factors Acquisition Job Aid or in more detailed HFE reference manuals.

HFE Process Tasks

The following process flow provides an outline and overview of key activities in the HFE process.

20. **Incorporate Human Factors Opportunities and Constraints into the Service Analysis**

    Using the results from the Shortfall Analysis, HFE identifies the human performance constraints and issues that need to be addressed or resolved, and provides them to the Service Analyses. This information may come from operations and maintenance analyses or concepts and other documents that may offer insight into the effects of HFE performance or cost constraints and limitations on the mission and system. Since most acquisitions are evolutionary, important HFE information may be obtained from predecessor or similar architectures, systems, or subsystem components. Analyses and tradeoff studies may be required to determine the effects of constraints and issues on

system performance. The existing literature and lessons learned databases should be reviewed in this case. (See *FAA Human Factors Integration Guide for Mission and Service Area Analysis*)

21. Incorporate Human Factors Requirements in Program Requirements

The preliminary, initial, and final program requirements documents contain functional, performance and supportability requirements that do not prescribe a specific solution. The requirements document defines the essential functional and performance capabilities and characteristics, including those involving the human component. As derived from the results of gap analyses and concepts of operation and maintenance, HFE provides for the requirements document the human performance factors (for example, in terms of task time, error rates, and throughput capabilities) and design compliance factors that impact system design and implementation. Cognitive, physical, and sensory requirements are established for the operator, maintainer, and support personnel that contribute to or constrain total system performance using detailed, vetted scenarios. Any safety hazards, health hazards, or critical errors that reduce job performance or system effectiveness must be defined. Staffing, training concepts, and resource limitations (e.g., staffing limits, allowable training time), including requirements for training devices, embedded training, and training logistics must also be described. (See *FAA Guidelines for Human Factors Requirements Development*)

22. Incorporate Human Factors Assessment in the Investment and Business Case Analysis

HFE provides the full range of human performance and interfaces (*e.g.*, cognitive, organizational, physical, functional, and environmental) to achieve an acceptable level of performance for operating, maintaining, and supporting the system. It provides these to the investment analysis and business case for each alternative being evaluated. (See Human Factors Assessments in Investment Analysis). The analyses provide information on what is known and unknown about human lifecycle costs and risks in meeting minimum system performance requirements. HFE areas relevant to the investment and business case analysis include:

- Human performance (human capabilities and limitations, workload, function allocation, hardware and software design, decision aids, environmental constraints, team-versus-individual performance)
- Training (length of training, training effectiveness, retraining, skill maintenance, training devices and facilities, embedded training)
- Staffing (staffing levels, team composition, organizational structure)
- Personnel selection (aptitudes, minimum skill levels, special skills, experience levels)
- Safety and health hazards (hazardous materials or conditions, system or equipment safety design, operational or procedural constraints, biomedical influences, protective equipment, required warnings and alarms)

23. Incorporate Human Factors Parameters in Program Baselines

The program baselines established at the initial and final investment decisions reflect the solution selected by the acquisition authority for implementation. Based on this solution, HFE inputs to the acquisition program baselines are those human performance requirements needed to achieve the required level of system performance. These inputs are derived from the specified system performance levels identified in program requirements documents (preliminary, initial, and final program requirements). They reflect a progressive refinement that provides increased definition, greater fidelity, and more specificity of relevant human-system performance characteristics. In order to properly incorporate these HFE inputs, the program engineers will need to identify constraints, limitations, and unique or specialized training requirements, staffing levels, or personnel skill requirements.

Also, to the degree possible, the required level of human and system performance must be based on practical measures of operational effectiveness and suitability and be stated in quantifiable terms (time to complete a given task, level of accuracy required, and throughput to be processed per unit time).

24. Designate Human Factors Coordinator for the Service Organization(s)

The Service Organization designates a Human Factors Coordinator to develop, direct, and monitor HFE activities during system acquisition. This designation needs to occur as early as possible during investment and business case analysis to ensure that human considerations are an integral element of market surveys, tradeoff analyses, and the definition of requirements for candidate solutions to mission need. The Human Factors Coordinator has the following responsibilities:

- Define human impacts and constraints during investment analysis and determine human-system functional, performance, and interface requirements,
- Evaluate human-system interfaces during market surveys, tradeoff analyses, and prototypes,
- Prepare and update HFE portions of program planning documents, procurement packages, evaluation and performance criteria/measures, and data collection efforts,
- Develop and analyze operational scenarios and human-system modeling and simulation for operators and maintainers,
- Review and assess HFE concepts and designs,
- Coordinate HFE efforts and workgroup activities, and
- Coordinate HFE with other system engineering disciplines.

These details may be documented in a Human Factors Integrated Program Plan.

25. Establish Human Factors Working Group

The Human Factors Coordinator may establish and chair a Human Factors Working Group (HFWG) or some other team to facilitate accomplishment of HFE tasks and activities. The composition of the HFWG is tailored to the needs of the acquisition program. Membership typically consists of key Service Organization system engineering members and specialists, with outside members participating as needed.

26. Incorporate Human Factors Strategy and Tasks into Program Implementation Strategy and Planning

The human factors strategy depends on the size, cost, and complexity of the system to be acquired, as well as the nature and complexity of the human-product interface. It is recommended that the HFE strategy address such factors as:

- Scope and level of HFE,
- HFE roles and responsibilities of organizations and contractors,
- Means for evaluating the human-machine interface and achieving user buy-in,
- Data sources and facilities needed,
- Distribution of funding and other resources,
- Timing and scope of HFE activities, and
- Relationship of HFE with other program elements.

The HFWG may assist in developing strategies appropriate for different types of acquisition programs, such as those that procure non-developmental items, commercial, off-the-shelf products, or fully developed new systems.

The human factors tasks and activities define the HFE work to be done during program implementation. For each task, the program planning documentation assigns the responsible person and organization, identifies any output and the approval authority, specifies when the task is to be completed, and allocates resources. As the program progresses through Solution Implementation (Section 0), the human factors portion of the program plan is updated to reflect changes in program strategy or execution and to provide more planning detail as it is developed.

27. Develop Integrated Human Factors Planning Information

For well managed system acquisition programs, the Service Organization prepares a Human Factors Plan or integrates human factors input to the SEMP. This information incorporates input from the various domains of human factors, such as training, staffing, personnel selection, and safety. Recommended content and format are outlined in *FAA Human Factors Acquisition Job Aid*. Tasks associated with this plan include:

- Defining the operational concept and support concept,
- Describing the target population,
- Defining human/system interfaces,
- Defining human impacts of the system,
- Defining the HFE strategy, and
- Defining HFE implementation tasks, activities, and schedule.

28. Incorporate Human Factors Requirements into System Statements of Work and Specifications

The System Statement of Work and Specifications translate human-system functional and performance requirements and appropriate HFE work tasks to the contractor in a clear, unambiguous, and contractually binding document. The Statement of Work contains all human factors tasking to be imposed on the contractor, and defines data deliverables in the Contract Data Requirements List (CDRL) and associated human factors Data Item Descriptions (DID). The System Specification addresses the following elements to ensure that required human performance effectively influences system design:

- Staffing constraints,
- Required operator and maintainer skills and skill level,
- Training time and cost for formal, informal, and on-the-job skill development,
- Acceptable levels of human and system task performance when operated and maintained by the target user and maintainer population, and
- Human-system interface requirements.

29. Include Human Factors in Source Evaluation Criteria

Human performance makes an excellent candidate as an evaluation factor in source selection (Section M of the SOW). By providing vendors a clear indication that the government attributes significant weight to how operators and maintainers perform with the system, the agency sends a strong message that operational suitability and effectiveness are of utmost importance.

30. Conduct HFE Analyses

The responsible Service Organization oversees, monitors, and reviews HFE analyses conducted by the implementation organization. These analyses may involve:

- Defining and allocating system functions and requirements (human factors requirements analysis, HCI prototyping, staffing analysis, training needs analysis, training effectiveness analysis),

- Analyzing information flow and processing (information requirement analysis, HCI design analysis),
- Estimating operator and maintainer capabilities (task performance analysis, training performance analysis, time and motion study, safety analysis),
- Defining and analyzing physical and cognitive tasks and workloads (task analysis, job design analysis, organizational design analysis), and
- Identifying and measuring human error risks and defining their mitigation and impact on design, equipment, procedures, and task performance (critical task analysis, human reliability analysis for Reliability, Maintainability, and Availability Engineering; human factors safety analysis; and human factors risk assessment).

31. Apply HFE to System Design

HFE is applied to system design activities to optimize human-system interfaces and to ensure that human performance requirements are satisfied. HFE is applied to the full scope of system design, including experiments, tests, and studies; engineering drawings; work environment, crew station, and facility design; performance and design specifications; procedure development; software development; and job aids, technical manuals and other documentation. The following are used effectively in defining human-product interfaces during system design:

- Prototypes and computer models,
- Three-dimensional mockups,
- Scale models,
- Static and dynamic simulation, and
- Early user evaluation.

32. Test System Against Human Performance Requirements

To determine if the system complies with human performance requirements, testing is initiated as early as possible in system development. HFE findings from design reviews, prototype reviews, mockup inspections, demonstrations, modeling, simulations, and other early engineering activities/assessments are used in planning and conducting later and more rigorous test and evaluation activities. HFE testing focuses on verifying that user personnel in the intended operational environment are able to operate, maintain, and support the system under normal and off-nominal operating conditions.

33. Incorporate Human Factors Considerations in Post-Implementation Review

Operational suitability and effectiveness are major evaluation factors that are considered in making the decision to place a new capability into operational service. Satisfactory human performance is an integral element of operational suitability and effectiveness. The broad range of HFE issues is addressed during this activity. Also, a plan is formulated to assess and monitor the human-system performance of the new capability following its deployment to the operational environment, especially for risks and limitations noted during the In-Service Review.

5.4.3 Outputs

Efforts to manage the HFE program, establish requirements, conduct system integration, and test and evaluate HFE compliance may result in many different HFE outputs and products. These products include human factors input to the primary acquisition documentation as well as human factors research, studies, and analyses that support program and design decisions and documentation. Examples of these products include human factors risk analyses, human factors benefits analyses, criteria for performance evaluation, prototype designs, and critical task analyses.

The HFE activities and their resultant products are described in more detail in the FAA Human Factors Acquisition Job Aid and other government and commercial HFE manuals, and are reflected in the following five key components of program planning and implementation.

HFE Planning Criteria

HFE planning involves developing detailed concepts of use, user and task analyses, HFE activity schedules, levels of effort, methods to be used, strategy for development and verification, and an approach to implementing and integrating with other program planning. This information is sent to Integrated Technical Management (see Section

4.1).

HFE Analysis Reports

HFE analysis involves identifying the best allocation of roles/tasks/requirements to personnel, equipment, software, or combinations to meet the acquisition objectives. It includes dissecting functions into specific tasks, analyzing tasks to determine human performance parameters and information requirements, quantifying task parameters to permit evaluation of human-system interfaces in relation to total system operation, and identifying HFE risk areas and safety hazards.

HFE Design and Development Analysis Reports

HFE design and development involves converting mission, system, and task analyses data into: (1) detail designs, and (2) development plans to create human-system information flow and interfaces that operate within human performance capabilities, meet system functional requirements, and accomplish mission objectives as assessed though trade studies (see Section 4.6: Information Management Process).

HFE Test and Evaluation Analysis Reports

HFE test and evaluation involves verifying that systems, equipment, software, and facilities may be operated and maintained within intended user performance capabilities and is compatible with overall system requirements, organizational design, operational tempo, and resource constraints (see Section 2.2.5.1: Product Realization and Section 4.7: Verification and Validation).

HFE Management and Coordination Analysis Reports

HFE management and coordination involves coordinating with and providing input to reliability, maintainability, and availability engineering; system safety; risk management; facilities and systems engineering; integrated logistic support; and other HFE functions, including biomedical, personnel selection, staffing, and training functions.

Additional Information

For sources of information used to generate content throughout this section, see References.

5.5 Information Security Engineering

Information Security Engineering (ISE) is a specialty engineering discipline within Systems Engineering (SE). The practice of ISE involves the analysis of threats and vulnerabilities to information systems and the assessment and mitigation of risk to the information assets that constitute the system during its lifecycle.

Federal legislation, such as the Clinger-Cohen Act of 1996, the Federal Information Security Management Act (FISMA) of 2002, and the Federal Information Security Amendments Act (FISAA) of 2012, establishes a clear legal basis for information security risk management of federal information technology (IT) resources.

FISMA creates a set of mandatory standards known as Federal Information Processing Standards (FIPS). FIPS Publications are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347). With the passage of the Federal Information Security Management Act of 2002, there is no longer a statutory provision to allow for agencies to waive mandatory FIPS.

There are two FIPS standards that define the Security Risk Management Process for the agency; FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and FIPS 200 Minimum Security Requirements for Federal Information and Information Systems. Taken together, these standards lay out the mechanisms for determining the appropriate security controls which a system must contain, the process for assessing the risk level of the system, and a lifecycle process that allows the appropriate FAA executives to understand, manage and reduce information security risk.

The FAA manages compliance with FISMA via FAA Order 1370.82A, Information Systems Security Program. It creates the governance structure for FISMA compliance by establishing the Security Authorization process. Under the Security Authorization process, all systems must be assessed for risk in accordance with FIPS 199 and FIPS 200 prior to becoming operational. Designated Authorizing Officials must accept any residual risk discovered during the Authorization process and the agency must track residual risk and develop mitigation plans, known as Plan of Action and Milestones (POA&M) for each residual risk, with the goal of reducing residual risk to the lowest possible level.

All systems are reassessed, at a minimum, on an annual basis. They are fully reauthorized by the Authorizing Official every three years. If a significant change occurs to the system they are immediately reevaluated. The authorization process is executed by an Information Systems Security Manager (ISSM), who interfaces with system owners, operates an independent assessment team and prepares documents and recommendations for the Authorizing Official. The agency maintains an Authorization Handbook, which provides additional details on the process. It is updated annually.

In support of timely and cost effective Security Authorizations, the FAA's Acquisition Management System (AMS) identifies steps for analyzing the Security Risk of an acquisition at each AMS phase. The FAA's Acquisition Management System (AMS) provides guidance and a flowchart of the steps to be conducted for ISE under the Security section at the FAST website. The FAA procedures and practices for conducting ISE continue to evolve. This ISE section provides system/security engineers and program managers useful references, steps, and processes for effectively integrating Information Security into systems being developed and deployed, emphasizing assessment and mitigation of information security risks and the need to start early in the acquisition lifecycle.

In performing ISE, systems and security engineers apply engineering principles to manage and control system security risk to the operational mission of the enterprise. The ISE process, outlined in the next section, defines the tasks that will produce effective and suitable management, operational, and technical security controls for an FAA system. ISE is conducted during all phases of the system lifecycle.

Security risk management, in conjunction with the security policies cited above, produces security requirements, which are statements of the implementation of mitigations to security risks that

need to be controlled or reduced. Implementing system design and security controls mitigates security risks to an acceptable level. Successful application of ISE combines control measures for prevention, detection, and recovery from security attacks that would compromise confidentiality, integrity, and/or availability of a system's IT assets. IT assets include both data and information.

The SE requirements management element (see Section 3.3: Requirements Analysis) is essential for defining and implementing security controls.

Several factors drive the need to perform ISE and to develop and implement rigorous security controls. Figure 56 illustrates these drivers:

- **Information Age Technology and Automation.** The FAA Acquisition Management System (AMS) calls for using or adapting commercially available IT products to satisfy the agency's mission needs. These COTS products may contain vulnerabilities that, unless properly identified, controlled, and managed, could cause unacceptable risks to FAA services, capabilities, and functions.
- **Critical Infrastructure and Homeland Security.** Homeland Security Presidential Policy Directive 8 (HS-PPD-8) establishes a national policy for Federal departments and agencies to identify and prioritize critical U.S. infrastructure and key resources and to protect them from terrorist attacks.
- **Aviation Growth, NAS Architecture and Operational Concepts.** The pervasiveness of networked information and the increased interconnectivity of FAA systems significantly broaden the agency's exposure to malicious activities from a variety of sources. Expanded services and capabilities that networking and automation have introduced enable improved performance and efficiency, yet dramatically expand vulnerabilities to systems' confidentiality, integrity, and availability unless FAA properly addresses security.
- **Rising Terrorist and National Threats.** FAA is modernizing its capabilities to ensure that the aviation transportation system is adequately protected from risks to the safety and security of the flying public. Information security supports homeland security, contingency response, and disaster recovery as services and capabilities of the NAS, which is a critical infrastructure for the United States.

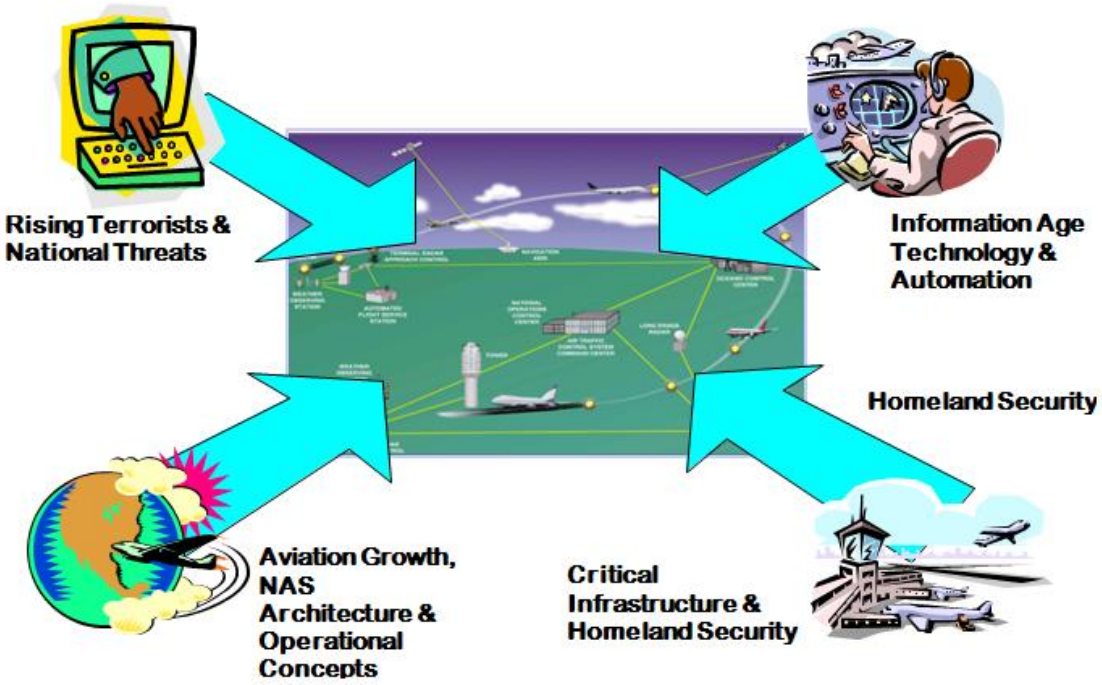


Figure 56: Factors Driving Security

These four factors drive FAA toward a more thorough and disciplined implementation of ISE throughout the system lifecycle. FAA programs that include security requirements early in development and acquisition typically have lower costs and more effective security features when compared to adding security controls later in the AMS lifecycle. The ISE process provides the information security risk management framework within the AMS, from early planning to contract closeout and/or system disposal.

5.5.1 Information Security Engineering Principles

Managing information system-related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization—from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning and managing projects, to individuals on the front lines developing, implementing, and operating the systems supporting the organization's core missions and business processes. Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization. Figure 57 illustrates a three-tiered approach to risk management that addresses risk-related concerns at: (i) the *organization* level; (ii) the *mission and business process* level; and (iii) the *information system* level.

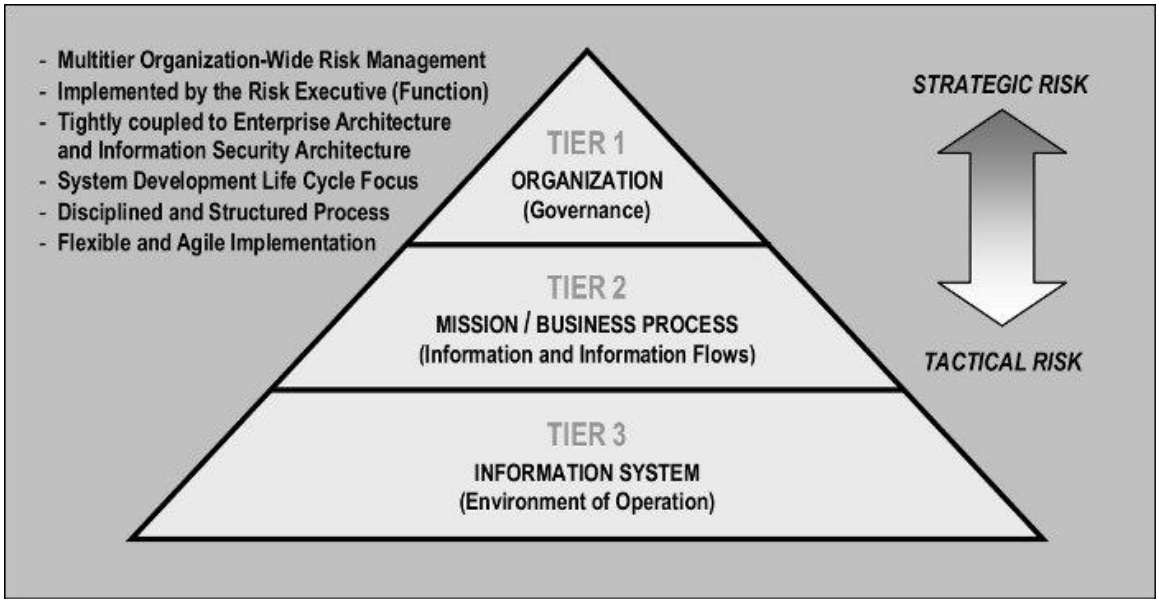


Figure 57: Tiered Risk Management Approach

ISE principles provide the foundation for a consistent and structured approach to designing, developing, and implementing information security capabilities that span the system, both logically and physically. Applying ISE principles at appropriate phases of the system lifecycle can provide information security, which is a system characteristic. There are a series of NIST Special Publications which provide the complete ISE guidelines for federal systems. Prior to undertaking the design, development and implementation of security controls, it is important to be familiar with the following NIST Special Publications:

- Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations
- Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans

In addition, NIST SP 800-27 (Rev. A) identifies 33 ISE principles that should be considered during different phases of the system lifecycle. These principles are applicable across the system lifecycle, as summarized in Table 29, where one check (✓) signifies that the principle can be used to support the lifecycle phase, and two checks (✓✓) signify that the principle is key to successful completion of the lifecycle phase.

Note: The National Institute of Standards and Technology (NIST) is a non-regulatory Federal Agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

Table 29: IT Security Principles (from NIST SP 800-27, Rev. A) Versus AMS Lifecycle

IT Security Principles (NIST SP 800-27 Rev. A)		Mission Analysis		Investment Analysis		Solution Implementation	In-Service	Disposal
#	Description	Service Area Analysis	Concept and Requirements Analysis	Initial	Final			
Security Foundation								
1	Establish a sound security policy as the "foundation" for design.	√√	√√	√	√	√	√	√
2	Treat security as an integral part of the overall system design.	√√	√√	√√	√√	√√	√√	√
3	Clearly delineate the physical and logical security boundaries governed by associated security policies.	√√	√√	√√	√√	√	√	
4	Ensure that developers are trained in how to develop secure software.	√√	√√	√√	√√	√		
Risk-Based								
5	Reduce risk to an acceptable level.	√√	√√	√√	√√	√√	√√	√√
6	Assume that external systems are insecure.	√√	√√	√√	√√	√√	√√	√
7	Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.	√√	√√	√√	√√		√√	
8	Implement tailored system security measures to meet organizational security goals.	√	√	√√	√√	√	√√	√
9	Protect information while being processed, in transit, and in storage.	√	√	√√	√√	√	√√	√
10	Consider custom products to achieve adequate security.	√	√	√√	√√	√	√	
11	Protect against all likely classes of "attacks."	√	√	√√	√√	√√	√	√

Ease of Use								
12	Where possible, base security on open standards for portability and interoperability.	√	√	√√	√√	√		
13	Use common language in developing security requirements.	√√	√√	√√	√√		√√	
14	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.			√√	√√	√	√√	
15	Strive for operational ease of use.	√	√	√√	√√	√	√√	

(Table continued from previous page)

Increase Resilience								
16	Implement layered security (Ensure no single point of vulnerability).	√	√	√√	√√	√	√√	√
17	Design and operate an IT system to limit damage and to be resilient in response.	√	√	√√	√√		√√	
18	Provide assurance that the system is, and continues to be, resilient in the face of expected threats.	√	√	√√	√√	√	√√	√
19	Limit or contain vulnerabilities.			√√	√√	√	√	
20	Isolate public access systems from mission critical resources (e.g., data, processes, etc.).	√	√	√√	√√	√	√	
21	Use boundary mechanisms to separate computing systems and network infrastructures.			√√	√√	√	√√	
22	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.	√	√	√√	√√	√√	√	
23	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.	√	√	√	√	√	√√	
24	Strive for simplicity.	√	√	√√	√√	√	√√	√
25	Minimize the system elements to be trusted.	√	√	√√	√√	√	√√	
26	Implement least privilege.	√	√	√	√	√	√√	
27	Do not implement unnecessary security mechanisms.	√	√	√√	√√	√√	√	
28	Ensure proper security in the shutdown or disposal of a system.			√	√		√	
29	Identify and prevent common errors and vulnerabilities.			√√	√√			

Design with Network in Mind								
30	Implement security through a combination of measures distributed physically and logically.			√√	√√	√	√	√
31	Formulate security measures to address multiple overlapping information domains.	√	√	√√	√√	√	√	
32	Authenticate users and processes to ensure appropriate access control decisions both within and across domains.	√	√	√	√	√	√√	
33	Use unique identities to ensure accountability.	√	√	√	√	√	√√	

Reducing information security risk to an acceptable level is a primary ISE principle, and in today's networked world, the concept of risk management is central to ISE. FAA defines information security risk as, "The combination of a threat, its likelihood of successfully attacking a system, and the resulting effects and harm from that successful attack." Mitigating these risks requires solid security risk management, which includes assessment, mitigation, monitoring, and control of security risks throughout the system lifecycle.

Based on FAA Order 1370.82A, the appropriate Authorizing Official (AO) determines the acceptable level of risk based on a carefully considered risk assessment. The DAA determines whether the benefit of connecting and operating the system outweighs the residual risk, which is defined as the combined likelihood of exploits and potential loss or damage to mission capability. The DAA determination considers the operational benefits of the system, the criticality of information, the threats and vulnerabilities, and effectiveness of system features and security controls in addressing security risks.

Integrating system security into the design involves using the following ISE principles (as a minimum) during system development:

- (#8) Address the operational environment of the system and the system's contribution to the FAA mission and services in security policy
- (#3) Delineate clearly the physical and logical boundaries to be governed by the associated system security policies
- (#6) Identify potential tradeoffs between reducing risk and increased costs or impacts to operational effectiveness and suitability
- (#2–#31) Participate during Investment Analysis to identify security concerns and issues, assess system alternatives, and analyze security risks in alternatives. This ensures that the alternatives protect against likely classes of attacks.
- (#28) Include consideration of security features and controls for continuity of operations and disaster response to ensure appropriate availability

Participation in the Investment Analysis phase can improve security requirement statements and avoid costly, specialized controls for security services that may be effectively handled by existing system features, such as management procedures, operational controls, or boundary protection systems/services. Figure 58 illustrates the benefit of early ISE involvement in the system lifecycle.

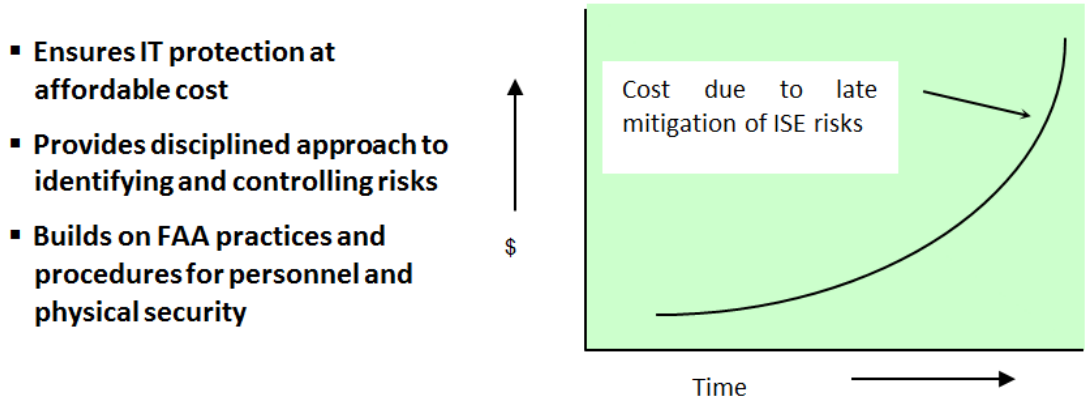


Figure 58: Benefits of Early Information Security Engineering

Security risk management applies to every AMS phase. The next section integrates guidance from NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* into the FAA Risk Management process model (see Section 4.3). NIST SP 800-37 divides the Information System Lifecycle into 6 distinct phases, as shown in Figure 59.

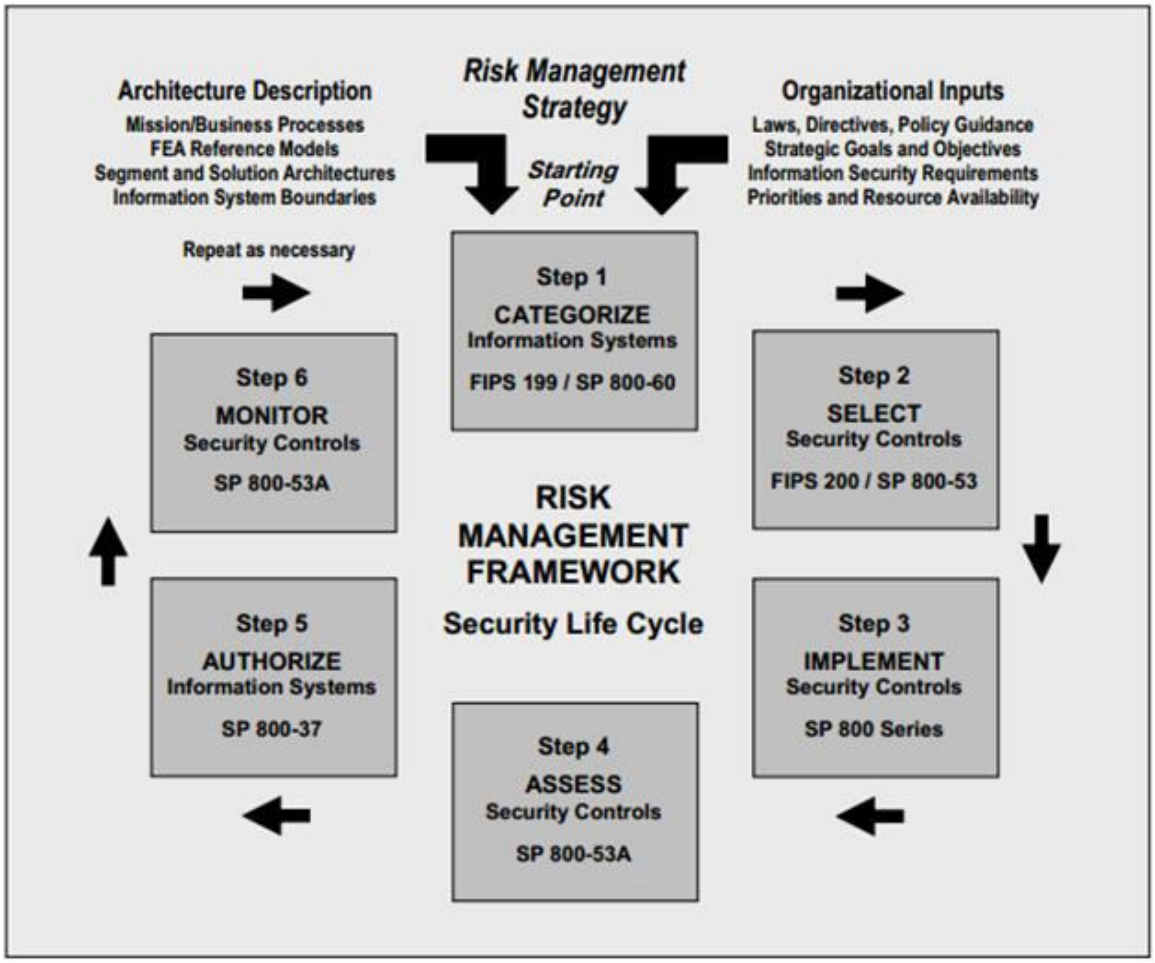


Figure 59: NIST Risk Management Framework Tasks

1. **Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis.22
2. **Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.23
3. **Implement** the security controls and describe how the controls are employed within the information system and its environment of operation.
4. **Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
5. **Authorize** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
6. **Monitor** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Table 30 indicates how risk management activities may be applied during the phases outlined in NIST SP 800-30, as well as the FAA AMS phases.

Table 30: Integration of Information Security Risk Management into AMS

Phases (NIST)	Phases (FAA)	Support from Risk Management Activities
Phase 1 Categorize	Service Analysis and Strategic Planning	Identified risks are used to select system risk level (low, moderate, high) which determines baseline security requirements. Security portion of the Concept of Operations (ConOps) is developed. System is evaluated to determine if special Privacy controls are required.
Phase 2 Select	Investment Analysis	The risks identified during this phase are used to support the security analyses of the system alternatives that may lead to architecture and design tradeoffs during downstream system development. Baseline requirements are tailored to the specific needs of the system environment, Common security controls are selected where applicable.
Phase 3 Implement	Solution Implementation	The security risk management efforts support assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks requiring mitigation must be made prior to system operation.
Phase 4 Assess	Solution Implementation and In-Service Management (including Technology Refresh)	The Authorization process is followed to prepare documentation and independent assessment is performed by the ISSM.
Phase 5 Authorize	In-Service Decision	The system is authorized by the Authorizing Official. Residual Risk is accepted and Plan of Action and Milestones (POA&M) are developed to plan for risk mitigation.
Phase 6 Monitor	In-Service Management Disposal	The system is annually reassessed and reauthorized every 3 years. POA&M closure activities are performed. Disposal guidelines contained in the Authorization Handbook are performed to ensure no risks are created by improper disposal of systems and data.

5.5.2 Inputs

As Figure 60 shows, several SE processes feed ISE. Functional Analysis, Requirements Management, Integrated Technical Planning, Interface Management, and Synthesis feed ISE with inputs, while Integrity of Analysis enables the ISE process. In turn, ISE provides output to other SE elements such as Functional Analysis, Requirements Management, and Risk Management. Note that ISE, like System Safety, conducts risk management separately from—yet it supports—Risk Management.

The ISE process outputs feed other SE processes, becoming integral to SE for the system lifecycle. The next section details the ISE outputs and products, while this section discusses the ISE products that result from applying the ISE principles.

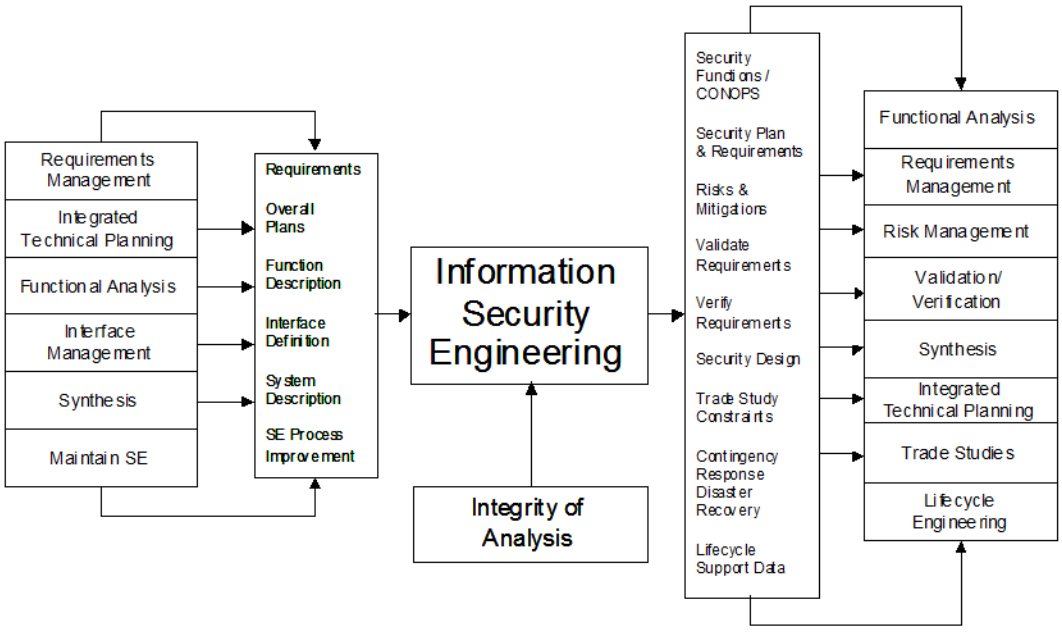


Figure 60: ISE Relationship to Other System Engineering Processes

5.5.3 Information Security Engineering Planning Process Activities

The ISE process tasks and activities support the phased AMS decisions, as shown in Figure 61. Each program or service organization shall tailor its ISE activities to meet its program milestones based on its System Engineering Management Plan (SEMP).

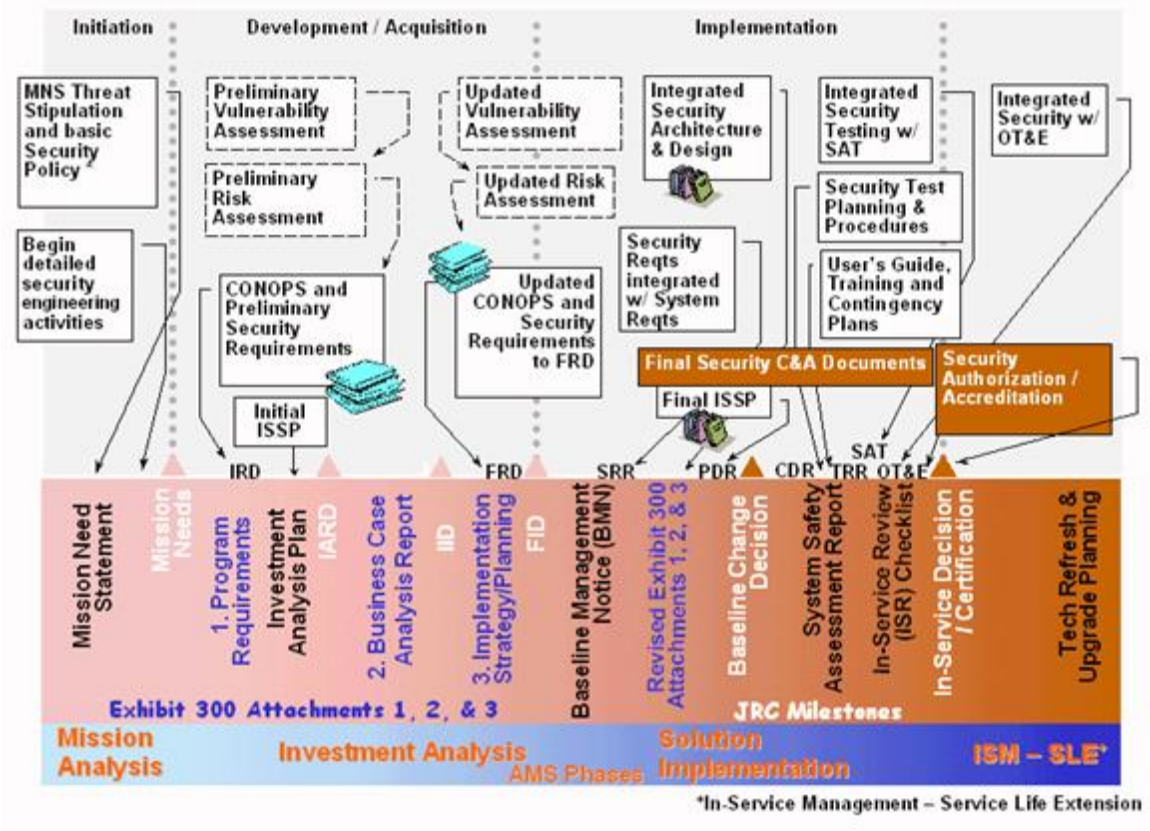


Figure 61: Security Activities during the AMS Phases

5.5.3.1 ISE Security Plan

NIST Special Publication 800-37 describes the development of a security plan for each information system. The security plan consists of the following documents:

- **Security Categorization**: The security categorization process is carried out by the information system owner and information owner/steward in cooperation and collaboration with appropriate organizational officials (i.e., senior leaders with mission/business function and/or risk management responsibilities). The security categorization process is conducted as an organization-wide activity taking into consideration the enterprise architecture and the information security architecture. This helps to ensure that individual information systems are categorized based on the mission and business objectives of the organization. The results of the security categorization process influence the selection of appropriate security controls for the information system and also, where applicable, the minimum assurance requirements for that system.
- **Information System Description**: Descriptive information about the information system is documented in the *system identification* section of the security plan, included in attachments to the plan, or referenced in other standard sources for information generated as part of the system development life cycle. Duplication of information is avoided, whenever possible. The level of detail provided in the security plan is determined by the organization and is typically commensurate with the security categorization of the information system. Information may be added to the system description as it becomes available during the system development life cycle and execution of the RMF tasks.
- **Information System Registration**: The registration process begins by identifying the information system (and subsystems, if appropriate) in the system inventory and establishes a relationship between the information system and the parent or governing organization that owns, manages, and/or controls the system. Information system

registration, in accordance with organizational policy, uses information in the system identification section of the security plan to inform the parent or governing organization of: (i) the existence of the information system; (ii) the key characteristics of the system; and (iii) any security implications for the organization due to the ongoing operation of the system. Information system registration provides organizations with an effective management/tracking tool that is necessary for security status reporting in accordance with applicable laws, Executive Orders, directives, policies, standards, guidance, or regulations. Those subsystems that are more dynamic in nature (e.g., subsystems in net-centric architectures) may not be present throughout all phases of the system development life cycle. Such subsystems are registered either as a subset of a well-defined information system or a method of registration for dynamic subsystems is implemented that includes as much information as feasible. Some information about dynamic subsystems is known prior to the subsystem manifesting itself in the information system (e.g., assumptions and constraints specified in the security plan). However, more detailed information may not be known until the subsystem manifests itself.

- **Common Control Selection**: Common controls are security controls that are inherited by one or more organizational information systems. Common controls are identified by the chief information officer and/or senior information security officer in collaboration with the information security architect and assigned to specific organizational entities (designated as common control providers) for development, implementation, assessment, and monitoring. Common control providers may also be *information system owners* when the common controls are resident within an information system. The organization consults information system owners when identifying common controls to ensure that the security capability provided by the inherited controls is sufficient to deliver adequate protection. When the common controls provided by the organization are not sufficient for information systems inheriting the controls, the system owners supplement the common controls with system-specific or hybrid controls to achieve the required protection for the system and/or accept greater risk. Information system owners inheriting common controls can either document the implementation of the controls in their respective security plans or reference the controls contained in the security plans of the common control providers.
- **System Control Selection**: The security controls are selected based on the security categorization of the information system. The security control selection process includes, as appropriate:

  (i) Choosing a set of baseline security controls;

  (ii) Tailoring the baseline security controls by applying scoping, parameterization and compensating control guidance;

  (iii) Supplementing the tailored baseline security controls, if necessary, with additional controls and/or control enhancements to address unique organizational needs based on a risk assessment (either formal or informal) and local conditions including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances; and (iv) specifying minimum assurance requirements, as appropriate. System Owners document in the security plan, the decisions (e.g., tailoring, supplementation, etc.) taken during the security control selection process, providing a sound rationale for those decisions. The security plan contains an overview of the security requirements for the information system in sufficient detail to determine that the security controls selected would meet those requirements. The security plan, in addition to the list of security controls to be implemented, describes the intended application of each control in the context of the information system with sufficient detail to enable a compliant implementation of the control. Information system owners can refer to the security authorization packages prepared by common control providers when making determinations regarding the adequacy of common controls inherited by their respective systems.
- **Monitoring Strategy**: A critical aspect of risk management is the ongoing monitoring of security controls employed within or inherited by the information system. An effective

monitoring strategy is developed early in the system development life cycle (i.e., during system design or COTS procurement decision) and can be included in the security plan. Monitoring strategy is currently implemented according to the guidance provided in the most recent Information Security Authorization Handbook.

The Security Plan, composed of these six documents, is a living document which should be started in Concept and Requirements Development (CRD) and updated throughout Investment Analysis. As additional details become available and design decisions are made, it should be updated.

5.5.3.2 ISE Activities in the AMS Life Cycle

Service Analysis & Strategic Planning, Concept &Requirements Definition

The ISE process starts in Service Analysis & Strategic Planning with a focus on the proposed system's operating environment, system boundaries, information assets and functions, data types, user types, special information privacy concerns and the potential threat and vulnerability sources to the system's information assets and functions. Basic system security policy flows from FAA organizational directives, such as FAA Order 1370.82A, as well as from FAA operating procedures and instructions.

The preliminary security plan and associated six documents are developed based on what is known about the system. At this phase, it is unlikely that specifics about networks, hardware of software are known, but boundaries, users and data types are of primary importance. Systems that contain privacy information, such as names or social security numbers, require extra scrutiny and close coordination with the FAA Privacy Office. Systems that will share information thru approved FAA boundary control systems with outside entities also require close coordination with the appropriate ISSM to ensure that common controls related to those boundary control systems are followed.

A system characterization should be performed during Concept and Requirements Development in coordination with the ISSM. A baseline set of security controls should be provided by the ISSM, which should be included in the preliminary requirements document. Any special security considerations that are known at this point, like privacy or the need for boundary control access, should be included in the system ConOps.

Investment Analysis

During Initial Investment Analysis, ISE analyzes the alternatives being considered by the investment analysis team for any relative differences in security risk and advices the investment analysis on possible tradeoffs which can reduce future risk. The NIST documents highlighted earlier, including NIST 800-27 can be especially helpful in this regard. The preliminary security requirements can be further tailored to fit the specifics of the system if it appears that the changes will be alternative neutral. The security section of the system CONOPS is further refined as additional details are known. If new privacy or external boundary needs are discovered, the ISE should notify the appropriate offices to evaluate if this will warrant a change in the overall system characterization chosen in CRD.

During the Final Investment Analysis phase, ISE refines and updates the security plan. During FIA, the requirements and general architecture are known to a better degree than during the alternatives analysis of the Initial Investment Analysis phase. Details about users, data types and boundaries should be clear and should be fully described in the security plan. The acquisition still consists of requirements at this phase, so specifics about hardware, software, operating systems and some network specifics may not be known, and this should be reflected in the security plan. These details will be added after acquisition when the security plan evolves into Authorization documents. Where ever possible, the ISE should format security plan elements in accordance with latest versions of the Authorization document templates to streamline the solution implementation work.

The ISE should ensure that the security requirements contained in the Final Program Requirements (fPR) document closely match the latest Authorization System Security Plan (SSP) template. Any delta between the FPR and the SSP Template generally reflects a requirement that

is newly added, was missed in an earlier phase, was removed since the pPRD or has excessively modified by the system owner. These deltas will result in a residual risk and POA&M in the final system.

The ISE should coordinate regularly with the ISSM on optional or mandatory common or hybrid security controls that the agency has designated. If a custom solution is planned that conflicts with a common or hybrid control that is mandated by an FAA policy, it could result in delays and additional costs related to changing the system or obtaining a policy waiver. It could also result in a POA&M.

During both phases of investment analysis, the ISE should always strive to include common or hybrid security control solution, as these are generally less expensive for the agency and permit common monitoring among many systems which reduces operational costs. The ISE should monitor new versions of the NIST publications as they are released to be in a position to anticipate how these might impact future versions of the security plan. The ISE should monitor the new version of the Authorization Handbook to anticipate how any changes might impact future activities.

Solution Implementation Phase

The ISE activities during solution implementation are explained in detail in the annual Information Systems Security Authorization Handbook. Separate versions are produced annually for both NAS and non-NAS systems. The activities and documents described in Section 5.5.4 generally occur during this phase.

In-Service Management Phase

The In-service Management Phase of the AMS is represented in the Information Security Authorization Handbook as the activities on the right side of Figure 60. The documents described below in Section 5.5.4 are updated on a regular basis to reflect the current state of each system in the FAA. The principal difference is in the use of the Annual Security Status Report form in place of the Executive Summary.

5.5.4 Information Security Engineering Authorization Process Activities

Figure 62 shows the FAA document process flow for security authorizations.

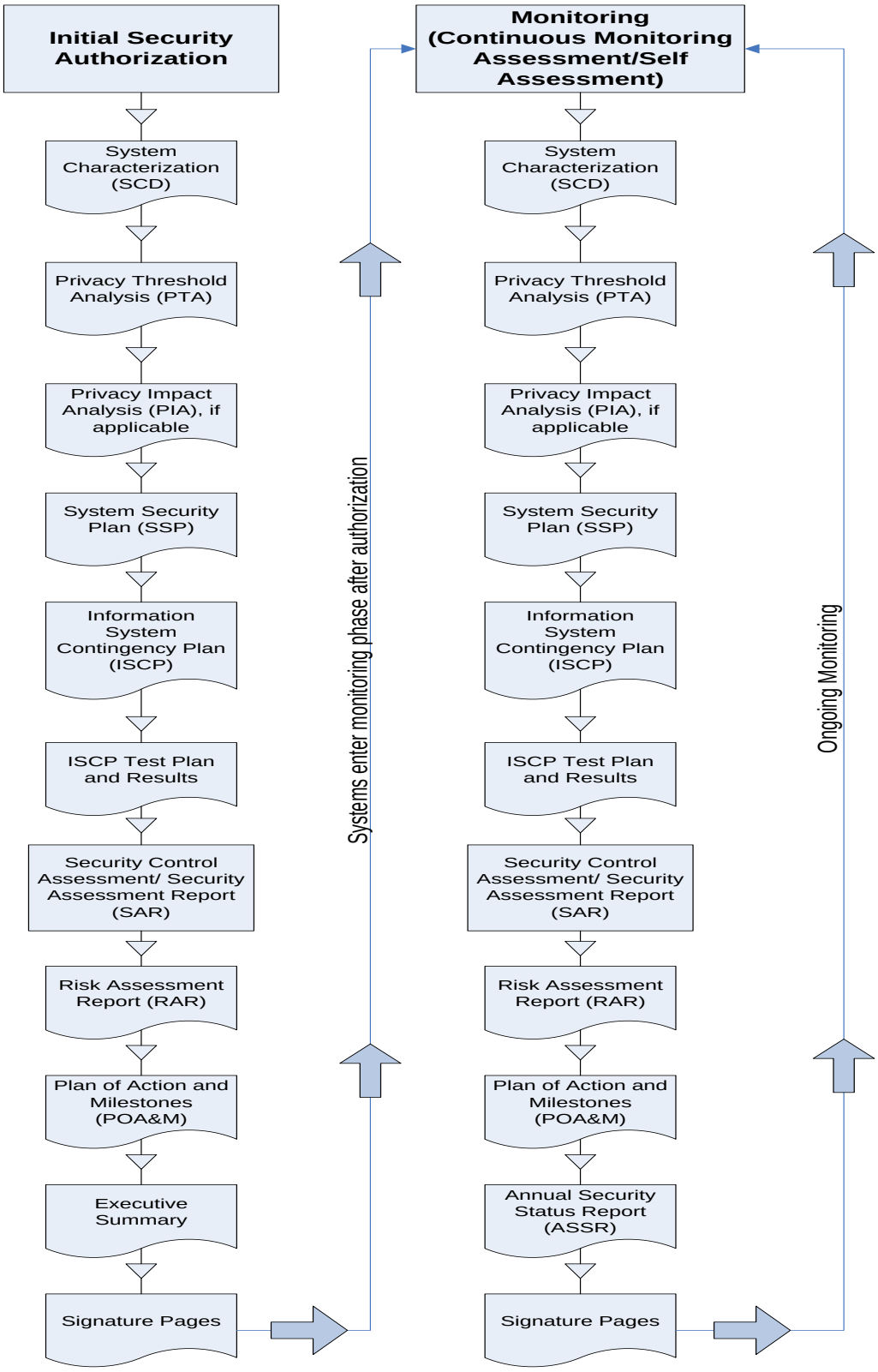


Figure 62: FAA Document Process flow for Security Authorizations

It is recommended that the ISE become fully familiar with the latest version of Authorization Handbook for the line of business that applies to the system under development. The following is a brief summary of each of the documents in the process flow for security authorizations:

System Characterization Document (SCD): The SCD is a living document and should be updated whenever a change occurs to the system. System information provided in the SCD is used repeatedly throughout the security authorization process and is frequently referenced in the key documents of the Security Authorization Package. The purpose of the SCD is to provide all system security related information in one document including:

- Identification of any future changes to the system
- Functional description of the system and its mission (including system architecture)
- Hardware and software/firmware assets
- Internal and external interfaces
- User interface(s)
- Security authorization boundary
- Security categorization analysis (Data types)
- e-authentication determination
- Privacy summary

The SO oversees, and is responsible for, the development of the initial SCD, as well as its maintenance throughout the life cycle of the system. The SCD is typically coordinated with, and receives input from, the Information Steward (IS), Information Systems Security Officer (ISSO), and the Information Systems Security Manager (ISSM) for the individual Line of Business (LOB) or Staff Office (SO) organization.

Privacy Threshold Analysis (PTA) and **Privacy Impact Analysis (PIA):** The FAA is responsible for protecting the privacy of personally identifiable information (PII), as the loss or theft of such PII could result in significant harm to the individual, the FAA, and its customers. FAA Order 1280.1B, Protecting Personally Identifiable Information (PII), December 17, 2008 (with changes effective 8/16/2011), sets forth the agency requirements for protecting PII and ensuring compliance with federal privacy laws, OMB mandates, and DOT and FAA privacy policies and procedures.

Privacy Threshold Assessment (PTA) - The PTA is used to assist in determining the need for privacy and other information collection compliance documentation for a particular system, business activity, program, information collection, and/or technology. A PTA is required for every IT system, rulemaking, or program's use of PII at the FAA. Additionally, the responses are used to alert other information asset stakeholders to the existence of a project/system so that they may identify any additional requirements relative to their area of responsibilities.

Privacy Impact Assessment (PIA) - Under the E-Government Act of 2002 (P.L. 107-347), system owners and developers are required to complete PIAs to determine the privacy implications of projects/systems that handle PII in an identifiable form. The adjudicated PTA is used to determine whether a PIA is required for your project/system.

System Security Plan (SSP): Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems supporting the operations and assets of the agency. This includes those provided or managed by another agency, contractor, or other source. System security planning is an important activity supporting system development. OMB Circular A-130 Management of Federal Information Resources requires all information systems to develop a System Security Plan (SSP). The SSP:

- Provides a summary of the information system security requirements.
- Identifies controls as being
  - System specific - Controls implemented solely by the system. (The responsibility of these controls lies with the SO and AO.)
  - Common - Controls inherited by one or more systems.
  - Hybrid - Partly common (inherited) and partly system specific controls.
- Describes the implementation of security controls in place (or planned for implementation) to meet those requirements.

- Delineates responsibility for security controls (common control provider, system specific, or hybrid – partial responsibility of common control provider/partial responsibility of system owner).
- Tailors controls and identifies compensating controls, as appropriate.

Information System Contingency Plan (ISCP) and **ISCP Test Plan and Results:** If the system under development is intended to be recovered at any point after a disruption occurs, an Information System Contingency Plan (ISCP) must be developed and periodically tested. The ISCP is used to recover the system at the original or an alternate location (NIST SP 800-34 pg 12 Table 2-2). The second contingency document is the Disaster Recovery Plan (DRP), which 'Provides procedures for relocating information systems to an alternate location' and is 'Activated after a major system disruption with long-term effects'. The DRP typically 'activates one or more ISCPs (800-34, Revision 1, Table 2-2). The updated guidance aligns to the updated NIST SP 800-53, Revision 3 controls, and incorporates contingency planning into the six steps of the RMF. An additional significant change to NIST SP 800-34, Revision 1 addresses testing, training and exercises based on FIPS 199 "availability" security objectives.

The ISCP details the procedures necessary to ensure the continuing performance of core business functions and services during an outage, and the restoration of any failed system functionality after an event. The ISCP is maintained and updated at least annually, based on system or personnel changes, or as a result of ISCP test plan testing for system authorization. The ISCP is not considered complete until it is tested and updated accordingly, based on the test results and lessons learned.

The ISCP test plan and results report describes the method used to test the ISCP and provides the results from one or more tests of the ISCP. The ISCP should be tested prior to implementation, so that the ISCP test results can be assessed as part of the initial assessment and authorization.

NIST SP 800-34, Revision 1 identifies two methods of testing an ISCP: *classroom (tabletop) and functional*. Classroom (tabletop) exercises, include all responsible parties, and are designed to have participants walk through the procedures without any actual recovery operations occurring. Classroom (tabletop) exercises are the most basic and least costly of the two types of exercises and are conducted before performing, or in conjunction with, a functional exercise. Functional exercises are more extensive, requiring the simulation of an actual event, focusing on one or more portions of the ISCP.

NIST SP 800-34, Revision 1 recommends the following guidelines for conducting test, training, and exercise (TT&E) activities appropriate to their respective impact level. It is an Office of Management and Budget (OMB) requirement to test the system at least annually.

- For low-impact systems, a tabletop exercise is sufficient. The tabletop should simulate a disruption, include all main ISCP points of contact, and be conducted by the system owner or responsible authority.
- For moderate-impact systems, a functional exercise should be conducted. The functional exercise should include all ISCP points of contact and be facilitated by the system owner or responsible authority. Exercise procedures should be developed to include an element of system recovery from backup media.
- For high-impact systems, a full-scale functional exercise should be conducted. The full-scale functional exercise should include a system failover to the alternate location. This could include additional activities such as full notification and response of key personnel to the recovery location, recovery of a server or database from backup media or setup, and processing from a server at an alternate location. The test should also include a full recovery and reconstitution of the information system to a known state.

Security Control Assessment (SCA) and Security Assessment Report (SAR)

As noted in NIST SP 800-37, Revision 1, the purpose of the SCA is to determine the extent security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system. The SCA provides a

snapshot in time of the security posture of both operational and developmental systems, utilizing data collected to evaluate existing system security controls (strengths) and lack of security controls (weaknesses). The assessment is generally conducted by an independent assessor or assessment team provided by the line of business ISSM.

Per NIST SP 800-53A, Revision 1, the primary purpose of the SAR is to convey the results of the security assessment to appropriate organizational officials. The SAR provides evidence to verify the adequacy of security controls and overall compliance with NIST SP 800-53, Revision 3. The SAR identifies weaknesses, provides recommendations for correcting any weaknesses or deficiencies noted in the controls. It also describes the general approach, the test steps, and any tools used for evaluating the effectiveness of applicable management, operational and technical baseline controls. NIST 800-53A, Revision 1 provides standardized methods and procedures for assessing the security controls.

Plan of Action and Milestones (POA&M) and Executive Summary

A POA&M is required by OMB Memorandum M-02-01 to provide a list of all vulnerabilities discovered during the RMF process, with recommended remediation actions (including risk acceptance and associated rationale), points of contact, required resources (including cost justification), and estimated dates for completion.

The System Owner oversees, and has primary responsibility for, reviewing and managing POA&M entries. Risk acceptance is the responsibility of the Authorizing Official.

The assessor, System Owner and ISSM must review the results of the security control assessment to determine the appropriate steps to address the weakness(es). The System Owner and designated officials may determine an assessment result identified as “Other than Satisfied” is inconsequential to the security of the system, and are candidates for risk acceptance. There may also be situations where a weakness exists but the system owner deems that remediation is not cost efficient or in some cases not possible without adversely impacting the system operations. In such cases the system owner should recommend the POA&M for risk acceptance to the Authorizing Official. Other findings may be determined to have an impact to the system and be considered for remediation. Their High, Medium, or Low risk level guides their prioritization.

In accordance with guidance in NIST SP 800-30, identified low-risk POA&M items are carefully examined to determine whether remediation action is required, or a risk acceptance recommendation is more appropriate. Even though the Authorizing Official also has the option to accept risk for a moderate or high-risk POA&M, NIST SP 800-30 recommends remediation based on a cost benefit analysis and system status (e.g., system will be retired within one year). Accepted risks are identified in the SSP control description for the target control.

Remediation tasks are tracked by the U.S. Department of Transportation (DOT), and status reports are provided at an aggregate level to OMB. Therefore, it is critical to record realistic and accurate information in each POA&M and commit to undertaking identified corrections of system weaknesses. The worksheet below contains specific methodology, guidance, and format for POA&M entries and provides a table for entering all of the required POA&M data in a single location. The POA&M information is included in the final Security Authorization Package as a part of the executive summary.

When the risk assessment process has been complete and the resultant risk acceptance/ remediation actions have been identified, the SSP is updated to reflect the POA&M items for each affected control, as well as those controls whose vulnerabilities have been risk-accepted. These controls are included as considerations in continuous monitoring and assessment activities.

Completion of the POA&M document permits the development of the security authorization executive summary and the submittal review process using the security authorization Work Flow checklist. Upon sign-off of the authorization documentation the approved POA&M information is recorded in the Cyber Security Assessment and Management (CSAM) tool.

The security authorization executive summary is a high-level description of the security of the system based on the results of the security authorization effort. The specific methodology,

guidance, and format of the initial security authorization executive summary are contained in the template.

NIST SP 800-137 defines Information system continuous Monitoring (ISCM) as “Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.” NIST notes that the terms continuous and ongoing in this context mean that security controls and organizational risk are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.

ISCM applies to all security controls implemented in organizational information systems and the environments in which those systems operate. It includes both automated and procedural (manual) methods. The continuous monitoring strategies, including frequency of security control monitoring and the rigor with which monitoring is conducted should be tailored; one size does not fit all. ISCM support the risk management process defined in NIST SP 800-39 by providing information to authorizing officials (AOs) for a range of potential risk decisions (i.e., accept, reject, share, transfer, or mitigate risk) in accordance with risk tolerance and mission/business priorities.

The objective is to support ongoing authorization of the system where the AO maintains sufficient knowledge of the current security state of the information system (including the effectiveness of the security controls employed within and inherited by the system) to determine whether continued operation is acceptable based on ongoing risk determinations, and if not, which step or steps in the Risk Management Framework needs to be re-executed in order to adequately mitigate the additional risk. Formal reauthorization actions are not necessary in situations where the continuous monitoring process provides the AO with the necessary information to manage the potential risk arising from changes to the information system or its environment of operation. Organizations maximize the use of status reports and security state information produced during the continuous monitoring process to minimize the level of effort required if a formal reauthorization action is required. Formal reauthorization can occur at the discretion of the AO. If a formal reauthorization action is required, the use of security and risk-related information produced during the continuous monitoring and ongoing authorization processes currently in effect, can be reused to support the reauthorization.

Systems completing the initial authorization or reauthorization process should enter the ISCM process. If a system breach occurs while in ISCM, the ISSM must determine whether the breach is serious enough to warrant a system reauthorization. Since system vulnerabilities have likely been exploited, a more in-depth risk assessment may be required in order to thoroughly evaluate known vulnerabilities and to identify previously unidentified vulnerabilities. It is likely new security controls, system modifications, and procedures will require implementation and/or modification to reduce the risk of future breaches, and all applicable system security authorization documentation must be updated accordingly.

All changes should be controlled by configuration management and control processes. For changes that may impact the security of the system, a security impact analysis must be performed. This will identify the security controls that the change may potentially affect. Using the results of the security impact analysis it should be determined whether the impact from the change warrants a reauthorization and full assessment, or does not require a reauthorization and can be dealt with a partial assessment targeting the change.

Even if there have not been changes to the system since the last assessment, the system documentation should still be reviewed for accuracy, especially in light of any POA&Ms that have been completed. Any changes should be reflected accordingly in the system documentation: SCD, SSP, PTA/PIA, ISCP, ISCP Test Results Report.

The information system security authorization decision is based on the composite assessment of controls over a three-year period, with a set of core security controls being assessed every year. All non-core controls are assessed at least once during the information system’s three-year authorization cycle. Figure 63 is an example of a system three-year assessment cycle. Core controls are assessed each year, and the remaining security controls are assessed over the three-year period. **“**Other Testing Results**”** represents the results from scheduled/unscheduled assessment results having occurred throughout the year, from maintenance actions, patch installations, continuous monitoring results, (such as SBCC and vulnerability scans), review of audit records, and other like events.

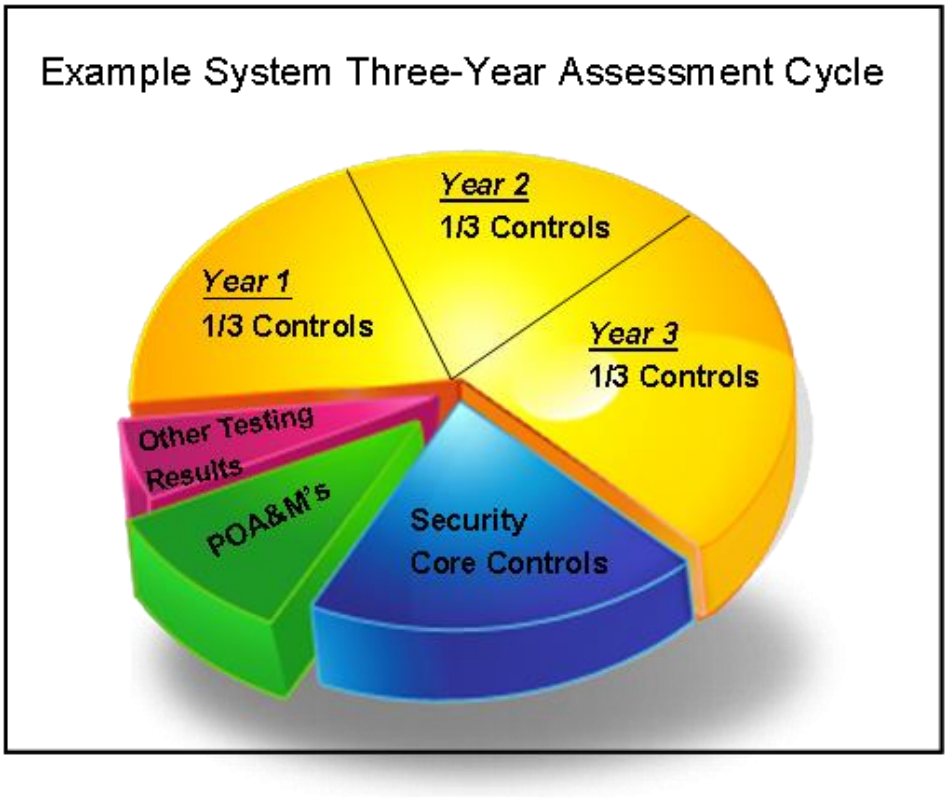


Figure 63: Three-Year Assessment Cycle

The SO/ISSM documents the core security controls and the non-core security controls assessment schedule using the FAA three-year Assessment Cycle Tracking Form.

Completion of "other testing results" activities (system upgrades, contingency plan, disaster recovery, maintenance activities, etc.), results for continuous monitoring activities, and POA&M assessments occurring throughout the three-year assessment cycle are noted on the FAA three-year assessment cycle tracking form. With the exception of those controls identified as core controls requiring assessment each year, the remaining controls will not require testing for the remainder of the three-year assessment cycle

The output of the 3rd year assessment will be the re-authorization of the system for another three year period. The FAA Three Year Assessment Tracking Form should be filled out and contain the security control assessment tracking for the three year authorization cycle. The Three Year Assessment Tracking Form should be maintained and attached to both the SAR and the Annual Security Status Report, so that the assessment status of the applicable security controls is readily available.

5.5.5 Outputs

The important aspect of security outputs/products is to embed security into the program products where possible to minimize treating security as a "standalone" component. The ISE process generates the following output and products.

Information System Security Plan (ISSP)

The system owner (Information Systems Security Certifier) shall initiate the ISSP during shortfall analysis. The ISSP evolves during the system's lifecycle, driven by the progression of system development. The ISSP is updated and revised based on ISE activities or other SE activities. To further guide planning, Table 31 relates the ISE activities and products to both the AMS milestone products and SE products. Analysis products outlined in the section below are used to update the ISSP.

Table 31: AMS Systems Engineering and ISE Relationships

AMS/SE Input	ISE Security Risk Management Activities	ISE Output or Product	AMS and SE Elements/Products Affected
Initial requirements, Initial functional architecture, Threat analysis criteria, OSA	Integrate Initial Security Needs and Threat Stipulation into the shortfall analysis	Statement of security policy and threat environment stipulation	New/updated shortfall analysis Draft pPR Initial investment analysis plan System Investment Analysis Review Requirements Management, Functional Analysis, Synthesis
ConOps, Initial requirements, analysis criteria, OSA	Develop ConOps and Preliminary Security Requirements	Initial Security requirements, ConOps	Business case analysis report Updated pPR for each alternative under serious consideration Initial investment analysis plan Acquisition strategy in the ISAP for each alternative under serious consideration Requirements Management, Functional Analysis, Conceptual functional architecture, Synthesis, ITP
FAA Policy, Standards, NAS Architecture, OSED, ConOps	Develop Preliminary ISSP (Including Basic Security Policy)	Preliminary ISSP with security policy statement	Final shortfall analysis ConOps Final Investment Analysis Plan Initial description of alternatives Requirements Management, Functional Analysis, RVCD, Trade Studies, Interface Management, SEMP
ConOps, Initial Functional Architecture, Functional Specification, Interface Control Documents, Initial VRTM, Stakeholder Needs	Develop Preliminary Vulnerability and Risk Assessment	Preliminary Vulnerability and Risk Assessment	fPR Final investment analysis report Final Exhibit 300 Final ISAP Requirements Management, RVCD, VRTM, OSED, Specialty Engineering, Risk Management, Validation, SEMP
ConOps, Initial Functional Architecture, Functional Specification, Interface Control Documents, Initial VRTM, Stakeholder Needs	Update the Vulnerability and Risk Assessment	Updated Vulnerability and Risk Assessment	SIR System Specification SOW CDRL Source selection criteria and plan Requirements Management, Specialty Engineering, Risk Management, Validation

AMS/SE Input	ISE Security Risk Management Activities	ISE Output or Product	AMS and SE Elements/Products Affected
ConOps, Initial requirements, analysis criteria, OSA	Update the ConOps and Security Requirements	Updated Security requirements, Updated ConOps	Requirements Management, Functional Analysis, Trade Studies, Interface Management, Configuration Management
ConOps, Final Security requirements	Integrate Security Requirements with System Requirements	Initial Verification Requirements Traceability Matrix, Interface Requirements Documents	System Requirements Review System Design Review – PDR Requirements Management, Integrated Technical Planning, Trade Studies, Synthesis, Interface Management, Configuration Management, Risk Management
Physical Architecture, Final Security Requirements, Design Analysis Report, Functional Architecture	Integrate Security Architecture and Design	Updated Physical Architecture, Functional Architecture	System Design Review — CDR System Capability Demonstration ITP, Requirements Management, Functional Analysis, Synthesis, Interface Management, Risk Management, Configuration Management
Physical Architecture, Functional Architecture, Risk Mitigation Plan, Updated Baselines, Updated ConOps, FAA Policy, Interface Control Documents, Program Risk Summary	Update the ISSP	Updated Information System Security Plan	ISAP Integrated Lifecycle Plan System Test Plan Operational Test & Evaluation (OT&E) Plan ITP, Specialty Engineering, Configuration Management, Lifecycle Engineering
Verification Requirements, Traceability Matrix, Risk Mitigation Plans, Interface Control Documents, Test and Assessment Articles, Physical Architecture, Functional Architecture, Functional Specification, Master Verification Plan	Develop Security Test Plans and Procedures	Security Test Plan, Security Test Procedures	System Test Plan OT&E Plan Integrated Technical Planning, Requirements Management, Interface Management, Verification, RVCD, VRTM

AMS/SE Input	ISE Security Risk Management Activities	ISE Output or Product	AMS and SE Elements/Products Affected
Trade Study Reports, Operational Services and Environmental Description, Functional Specification, Government and International Regulations and Statutes, FAA Policy, Requirements	Develop User's Guides, Training, and Contingency Plans	Contingency and Disaster Recovery Plan, User's Guides, Security Awareness Training (see 4.14)	Integrated Lifecycle Plan Functional Configuration Audit Physical Configuration Audit Functional Analysis, Configuration Management, Trade Studies, Specialty Engineering, Verification, ITP
Updated Verification Requirements Traceability Matrix, Requirements Verification Compliance Document, Verification Criteria, Updated Master Verification Plan	Conduct Security Testing	Updated Risk Mitigation Plan, Security Test Report	Test Readiness Review Qualification Test Final Acceptance Test Site Acceptance Test Verification, Integrated Technical Planning, Requirements Management, Configuration Management, Risk Management
Risk Mitigation Plan, Program Risk Summary, Updated ISSP, Contingency Plans, Test Validation Reports,	Create Final Security C&A Documents	Certification Package	In-Service Review Checklist OT&E Report Specialty Engineering, Configuration Management, Synthesis, Risk Management
Certification Package, FAA Management Decisions, Government and International Regulations and Statutes	Obtain Security Authorization/ Accreditation	Finalized Certification Package	Specialty Engineering, Configuration Management, Synthesis, Risk Management
Validated Need, Stakeholder Needs, Integrated Lifecycle Plan, Updated Acquisition Program Baseline, External Environmental Forces	Prepare for Tech Refresh and Upgrade Planning	Updated Security Requirements, Updated Security Certification Package, Updated Vulnerability and Risk Assessment	Lifecycle Engineering, Trade Studies, Configuration Management, Risk Management, Functional Analysis

Analysis Products

The risk assessment methodology described in this section guides collection of security analysis results and recommendations into products that support security accreditation of the service/domain/system. This methodology illustrates how ISE work products are used to validate and verify the security requirements of a given system. The work products are generated according to the individual ISSP for each FAA service / domain / system. Figure 64 indicates the type of closed-loop security risk management that is applied during the AMS phases. A similar loop applies to non-NAS projects as well.

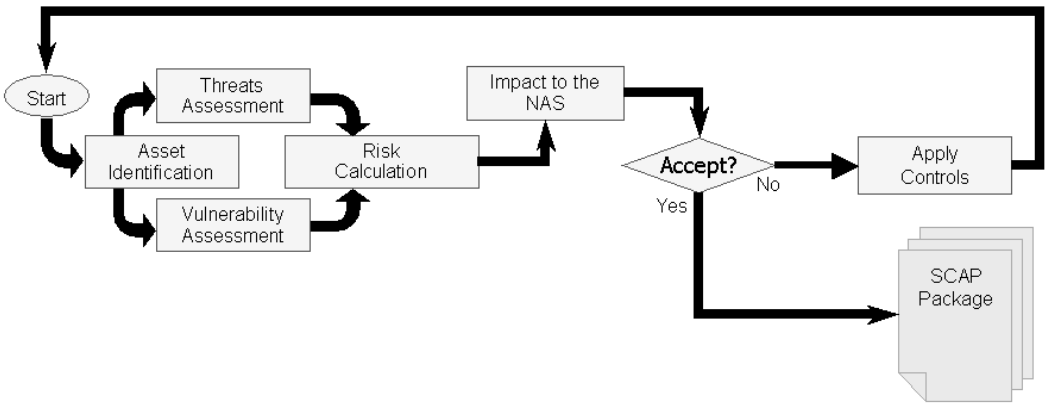


Figure 64: Closed-Loop Security Risk Management

This closed-loop method of risk management supports the FAA risk management process model described in Section 4.3: Risk Management, as shown in Figure 65.

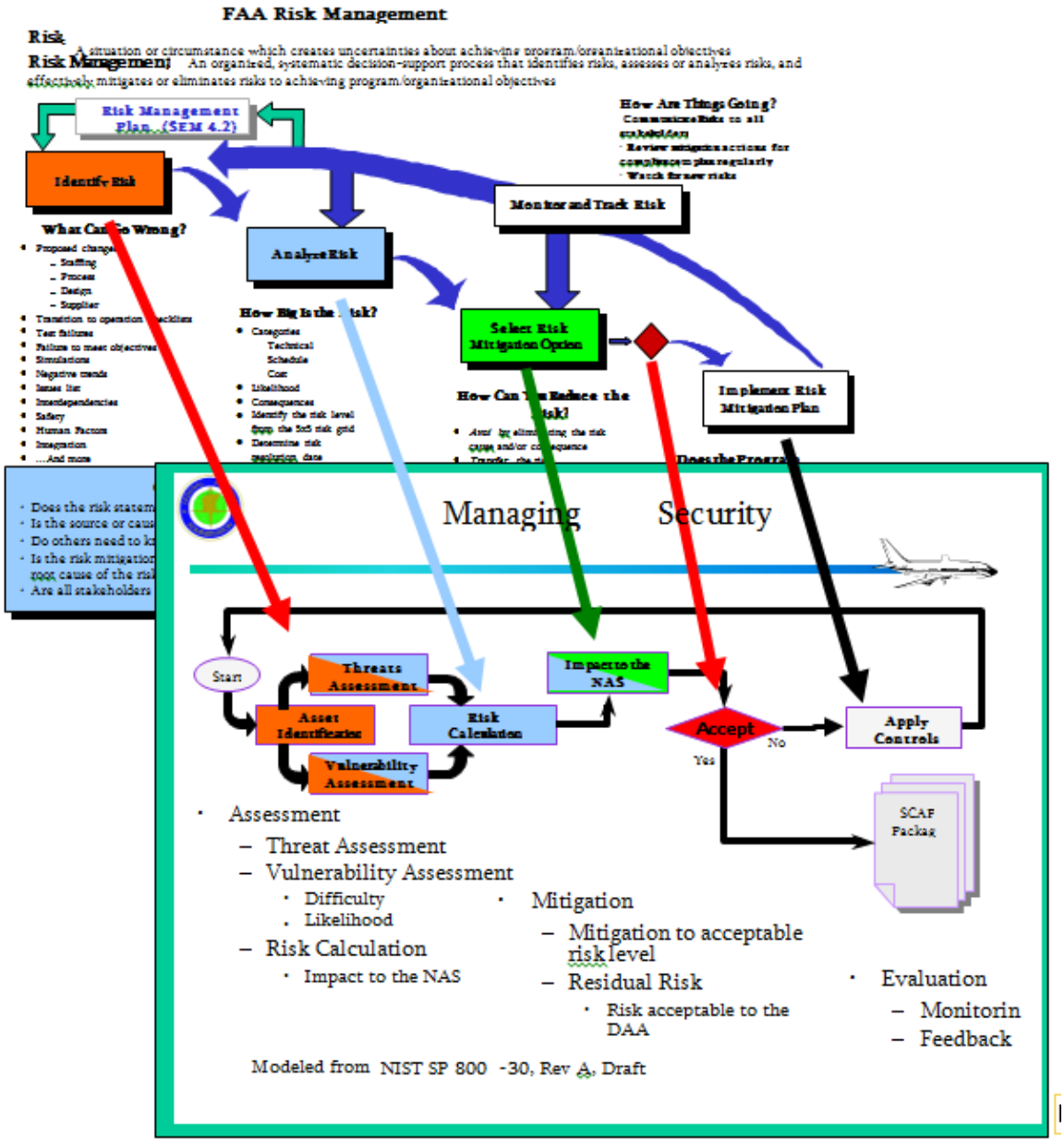


Figure 65: Correlation of Information Security Methodology with FAA Risk Management Model

The ISE Risk Assessment Matrix in Figure 66 can be used to analyze individual security risks. The matrix reflects the level of risk associated with the **likelihood** of a given threat source exploiting a given vulnerability and the **impact** of that threat source successfully exploiting the vulnerability. Risks to IT systems arise from events such as, but not limited to, the following:

- Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
- Unintentional errors and omissions
- IT disruptions due to natural or man-made disasters
- Failure to exercise due care and diligence in the implementation and operation of the IT system

To use the matrix, apply the determined **likelihood** value generated for each threat-vulnerability pair and apply the **impact** rating, considering the vulnerability is successfully exploited. Locate the **likelihood** value in the vertical column and the **impact** rating in the horizontal column. The **Risk Level** is where the two values intersect.

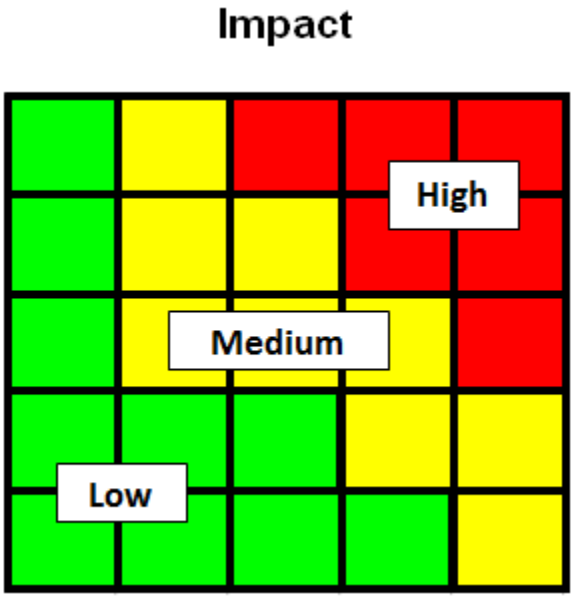


Figure 66: ISE Risk Assessment Matrix

Information Security Engineering Tools

There is not a specific set of tools for use in implementing Information Security. Tools should be chosen based on the desired final products and interoperability with other tools used in other SE elements. Tools can be used for discovering vulnerabilities, performing risk assessments, and for tracking and reporting the status of security controls.

Information Security Engineering Metrics

Security requirements should be implemented as early in a program as possible to avoid reworking the program after security requirements are introduced. This can be measured by reviewing the program to see if it meets these standards and that the requirements are implemented. This can be accomplished by ensuring security requirements are included in the plans of action and milestones (POA&M). Guidance for developing these metrics is in NIST Special Publication 800-55, *Performance Measurement Guide for Information Security*.

Additional Information

For sources of information used to generate content throughout this section, see References.

5.6 System Safety Engineering

System Safety Engineering (SSE) is a Specialty Engineering discipline within systems engineering (SE). It is required that system/safety engineers and program managers refer to FAA's Safety Management System (SMS) Manual and the Safety Risk Management Guidance for System Acquisitions (SRMGSA) for detailed information about planning and conducting SSE. The following paragraphs describe how SSE is integrated into a system's overall SE.

5.6.1 Definition

SSE is the application of engineering and management tools—including principles, criteria, and techniques—to optimize the safety of a system within the program's operational and programmatic constraints. These tools are used to identify, evaluate, and control hazards associated with a system. A hazard is any real or potential condition that can cause injury, illness, or death to people; damage to, or loss of, a system (hardware or software), equipment, or property; and/or damage to the environment. SSE's goal is to identify proactively the hazards in a system early, to continuously assess the risk (severity and likelihood) of each hazard, and to actively control the highest risk hazards. The SRMGSA provides more information on this topic.

As illustrated in Figure 67, the SSE process uses a closed-loop method of Safety Risk Management (SRM) to identify and mitigate risk in the NAS. The SRM process is divided into five phases:

1. Describe the system
2. Identify hazards
3. Analyze risk
4. Assess risk
5. Treat risk

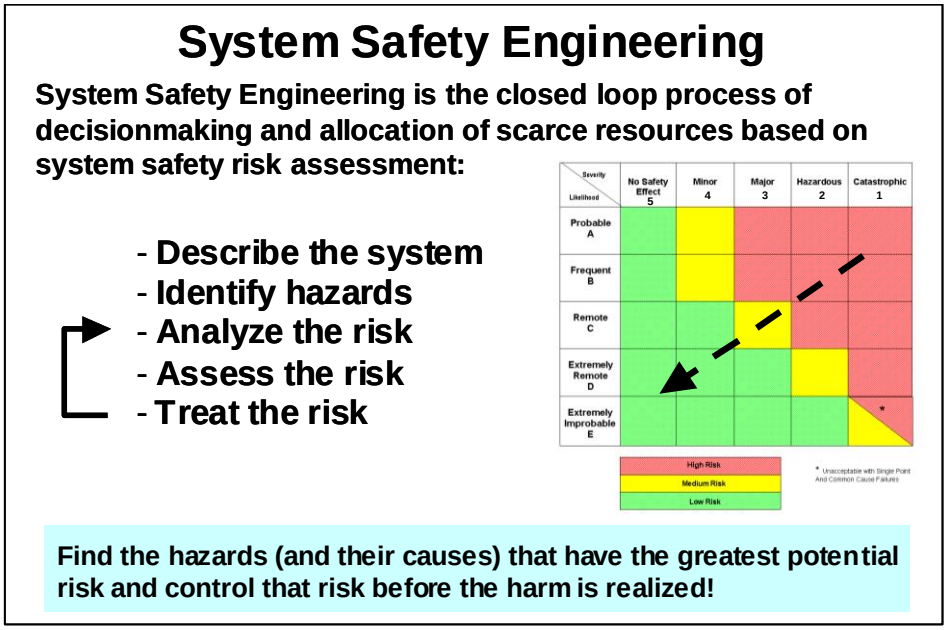


Figure 67: Closed-Loop Method of System Safety Engineering

The following documents describe how SSE is conducted in the FAA:

- FAA SMS Manual
- SRMGSA

The **FAA SMS Manual** is an integrated collection of principles, policies, processes, procedures, and programs used to identify, analyze, assess, manage, and monitor safety risk in the provision of Air Traffic Management (ATM) and Communication, Navigation, and Surveillance (CNS) services. It is a continuous, formalized, and proactive approach to system safety.

The SMS addresses the safety of all aspects of ATM and CNS services, including, but not limited to, airspace changes, changes to current operational procedures and standards, new and modified equipment (hardware and software), and associated human interactions. The SMS also addresses existing ATO operations, equipment, and behaviors in the NAS. To help ensure NAS safety, the SMS mandates the collection and analysis of safety data; the use of safety reviews, audits, and evaluations; the investigation of air traffic incidents and accidents; and the continuous monitoring of data.

The ATO uses its SMS to promote a positive safety culture through policies that align safety goals with organizational practices, employee training, voluntary reporting, and best practices.

The **SRMGSA** is the required guide for applying Safety Risk Management (SRM) to acquisitions that affect the NAS. The SRMGSA serves as:

- SMS guidance for acquisitions during these phases of the AMS cycle: Service Analysis, Concept and Requirements Definition (CRD), Investment Analysis (IA), Solution Implementation (SI), and In-Service Management.
- Specific guidance for system changes.
- A definition of the Investment Decision Authority's (IDA's) expectations regarding SRM.

The SRMGSA provides a framework and further process definition to ensure the execution of SRM throughout the entire lifecycle of a system or product.

Figure 68 shows what safety analyses are performed, relative to the phases of the AMS. These analyses are timed to best support the phased needs and decisions in the overall AMS process.

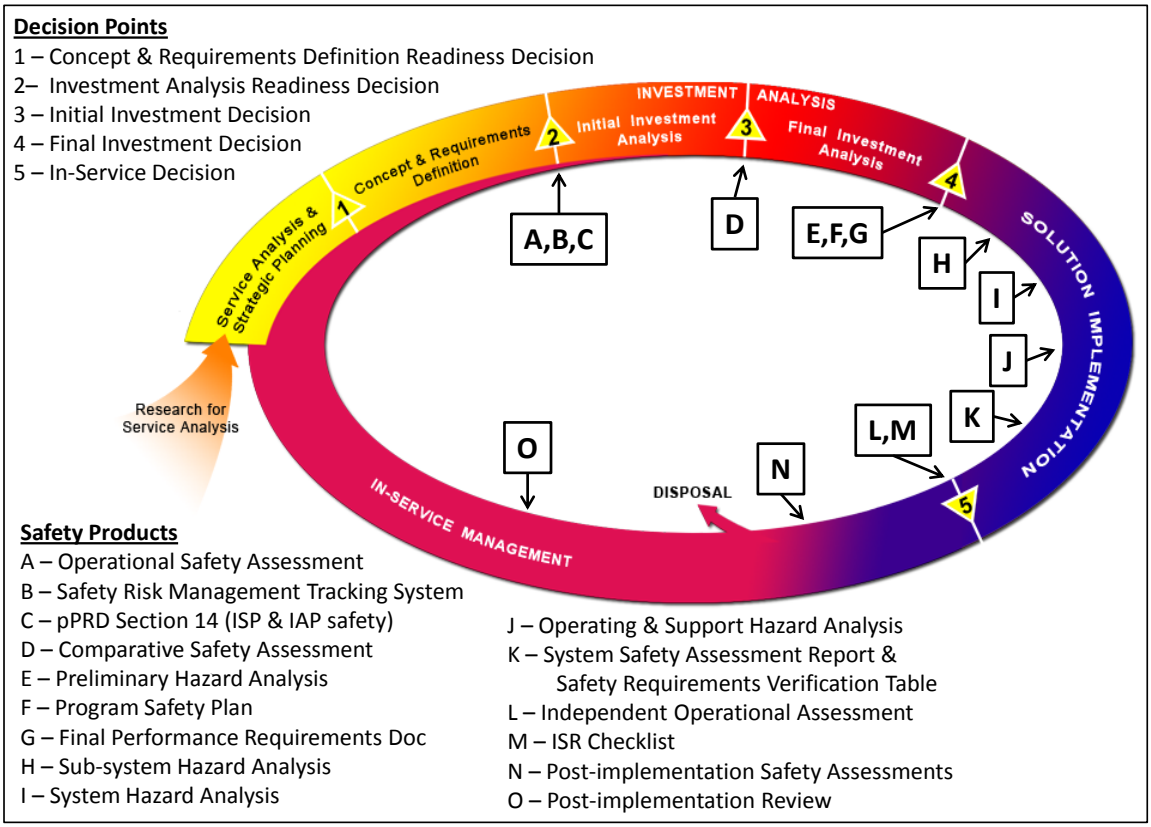
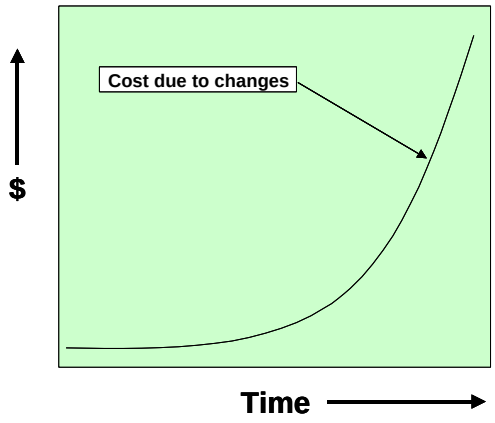


Figure 68: Types of Safety Hazard Analyses and their Relative Position in the FAA AMS

Performing SSE on a program optimizes the safety of a system by identifying, evaluating, and controlling hazards. SSE is also performed to:

- **Comply with FAA orders, the SMS, and AMS direction.** FAA's primary role is to ensure the safety of the NAS. Thus, the agency has issued FAA Order 8040.4, which directs all agency organizations to employ safety risk management in decision making. The safety risk management sections of the FAA SMS Manual present the methodology to comply with the order. Additionally, AMS policy, in accordance with FAA Order 8040.4, requires programs to perform system safety and to report the system safety program status at all decision points and investment reviews. The SRMGSA and the AMS provide more information on this subject.
- **Reduce total cost of development.** SSE reduces safety risk very early in a program's lifecycle, thus reducing cost and programmatic risk while also improving system integration and SE overall. This approach also has a positive effect on system performance and the overall schedule. As Figure 69 shows, the earlier in the lifecycle a problem is found and managed, the easier and less expensive it is to correct.
- **Improve program integration.** Outputs of the system safety process feed other SE processes, which improves the system's overall SE (Figure 70).

- **SSE finds and controls risks early**
- **Data-driven decisions**
- **System Engineering: requirements, risk, configuration, alternatives, interfaces, verification**
- **Program baseline is developed knowing the risks ahead of time**



System Safety Engineering reduces program cost and increases probability of program success!

Figure 69: Benefits of System Safety Engineering

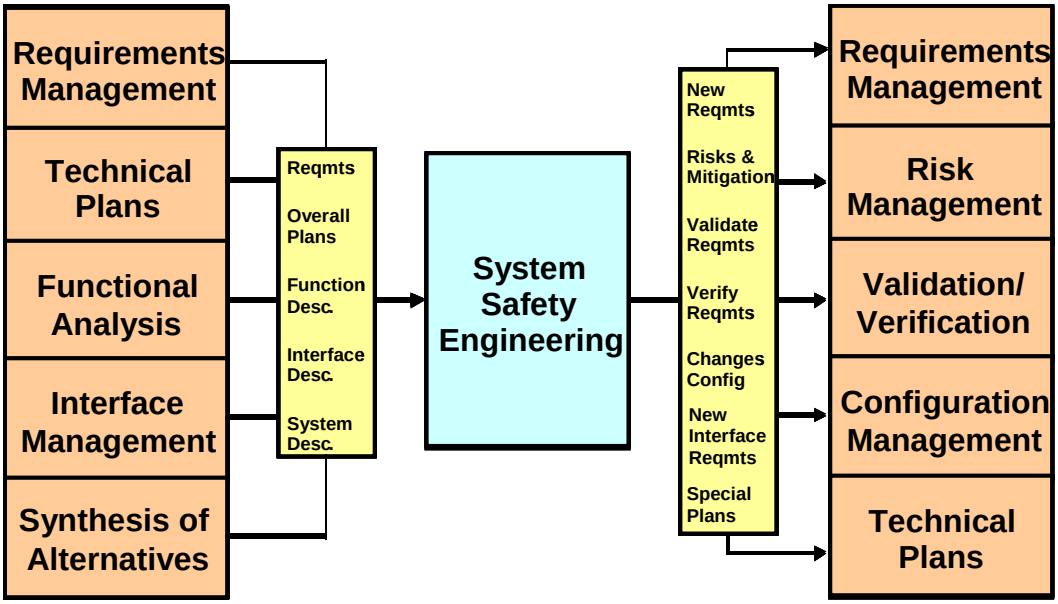


Figure 70: System Safety Engineering's Relationship to Other System Engineering Processes

5.6.2 System Safety Engineering Process Tasks

SSE follows the process tasks outlined in “General Specialty Engineering Process Tasks”. These general tasks correlate directly with the specific SSE tasks in Table 32 and, as previously stated, appear in the FAA SMS Manual and SRMGSA.

Table 32: General Specialty Engineering Tasks Correlated to SSE Tasks

General Specialty Engineering Process Tasks	Specific SSE Process Tasks
Obtain or develop an OSED	**Describe the system** • Define scope and objectives • Define Stakeholders • Identify criteria and plan for safety risk management effort (including any modeling/simulation potentially required) • Describe system/change (use, environment and intended function; including future configuration)/current safety issue
Bound the problem and define constraints on the study and design	
Select analytical methods and tools	
Analyze system parameters to determine system attributes	**Identify hazards** • Use structured approach • Be comprehensive (and do not dismiss hazards prematurely) • Employ lessons learned and experience supplemented by checklists
	Analyze the risk • Identify existing mitigations/controls • Determine risk outcome(s) • Provide quantitative data (preferred) or qualitative assessments
	Assess the risk • Rank, characterize, and prioritize hazards according to the severity and likelihood of their risk
Define and document Specialty Engineering requirements	**Mitigate the risk** • Identify feasible mitigation options • Develop risk treatment plans • Define performance targets for each hazard • Develop a monitoring plan • Implement and verify the implementation of mitigations • Record, monitor, and track to completion of monitoring plan • Verify predicted residual risk
Coordinate results with stakeholders	
Document the Specialty Engineering analysis in a Safety Risk Management Document (SRMD)	

5.6.3 Outputs

The following products are SSE outputs.

Program Planning

Per the SRMGSA, each program has to have a Program Safety Plan (PSP) which is the overall plan for conducting system safety management in the AMS. It is recommended that individual programs, when developing a program-specific PSP, consult the SRMGSA, which also develops the requirements for the program vendor's or contractor's System Safety Program Plan (SSPP).

Analysis Products

Table 33 lists the Safety Risk Management (SRM) products done within the AMS and where further information may be found.

Table 33: Products of System Safety Engineering

System Safety Process Products	Reference
Research and Systems Analysis (RSA) phase	SRMGSA sections on the RSA phase safety products
Operational Safety Assessment (OSA)	SRMGSA
Comparative Safety Assessment (CSA)	SRMGSA
Preliminary Hazard Analysis (PHA) {for AMS-related assessments}	SRMGSA
Hazard Analysis Worksheet (HAW) (for operations-related assessments)	SRMGSA
Program Safety Plan (PSP)	SRMGSA
System Safety Program Plan (SSPP)	SRMGSA
Subsystem Hazard Analysis (SSHA)	SRMGSA
System Hazard Analysis (SHA)	SRMGSA
Operating and Support Hazard Analysis (O&SHA)	SRMGSA
System Safety Assessment Report (SSAR)	SRMGSA
Safety Risk Management Tracking System (SRMTS)	SMS Manual SRMGSA
Safety Requirements Verification Table (SRVT)	SRMGSA

5.7 Hazardous Materials Management, Environmental Engineering, and Environmental, Occupational Safety and Health

Hazardous Materials Management/Environmental Engineering (HMM/EE) is the subset of Specialty Engineering concerned with identifying and mitigating the impacts both of the program on the environment and of the environment on the program. Environmental, Occupational Safety and Health (EOSH) requirements integration is a process applied within the FAA Systems Engineering (SE) process that ensures a program's ongoing compliance with applicable EOSH and sustainability (energy and water conservation) requirements. Federal, state, and local agencies have established mandates that regulate program impacts on the environment, occupational safety and health, and energy and water conservation. These mandates include requirements to manage hazardous materials, safeguard natural resources including ambient air, water, and land-based resources, and protect personnel from workplace hazards. FAA orders and directives (e.g., FAA Order 1050.10C, Prevention, Control, and Abatement of Environmental Pollution at FAA Facilities) relate federal EOSH regulations to FAA activities and also provide additional EOSH requirements specific to NAS operations. Conversely, environmental impacts on programs vary, depending on site-specific environmental conditions that may affect FAA operational requirements. The following sections describe the purpose and general process of HMM/EE and EOSH within SE.

5.7.1 Definitions

HMM/EE and EOSH are the mechanisms applied within the SE process to ensure a program's ongoing compliance with applicable EOSH regulations and requirements. Compliance with various EOSH regulations is required throughout a program's lifecycle, requiring early and continuous application of HMM/EE and EOSH principles. Key considerations are pollution prevention, occupational safety and health, cultural and natural resource conservation, public participation, and energy and water conservation. Through HMM/EE and EOSH, the breadth of environmental, occupational safety and health, and sustainability requirements are continuously monitored and considered to ensure that FAA's programs take the steps necessary to maintain compliance.

Additional issues concerning the applicability of state and local EOSH requirements to federal acquisitions should be referred to the Office of the Chief Counsel for an evaluation of supremacy clause and sovereign immunity implications. For example, the Resource Conservation and Recovery Act (RCRA) establishes standards for managing and disposing of hazardous wastes that result from various processes during program operation, and at the end of the program's lifecycle. These requirements may be administered through state agencies.

HMM/EE is also the SE process designed to provide early, pre-deployment planning and coordination to minimize the negative impacts that site-specific environmental conditions may have on a program's operability. HMM/EE processes highlight the impacts that environmental conditions and site-specific characteristics may have on a program. FAA specifications are the primary tool developed for various types of equipment to delineate operating conditions that shall be considered during the program's developmental stages. For example, the general FAA specification for electronic equipment, FAA-G-2100, details the design standards that shall be followed to ensure equipment functionality in environmental conditions of both seismic zones and temperature extremes. HMM/EE verifies that similar standards are considered and followed in the SE process to ensure the reliability of systems fielded under unique environmental settings.

HMM/EE and EOSH processes are performed to:

- Support reliable, safe, and sustained NAS operations;
- Ensure compliance with FAA, federal, state, and local environmental and occupational safety and health requirements;
- Ensure EOSH considerations are included in the acquisition management process;
- Track the status of EOSH issues with new and existing systems; and

- Minimize cost and schedule risks through early detection of EOSH issues, and inclusion of EOSH costs in the program baseline.

FAA Acquisition Management System (AMS) policy and guidance requires consideration of EOSH and sustainability requirements in the acquisition process. These requirements are described in the following AMS Sections:

- AMS Policy Section 3.6.3: Environment, Conservation, Occupational Safety, and Drug-free Workplace
- AMS Guidance Section T3.6.3: Environment, Conservation, Occupational Safety, and Drug Free Workplace (specific sustainability requirements)
- Policy Section 4.8, Environmental, Occupational Safety and Health, and Energy Considerations.

In addition, FAA has mandated compliance with applicable EOSH regulations through various Orders (e.g., FAA Order 1050.17, Airway Facilities Environmental and Safety Compliance Program, FAA Order 3900.19B, FAA Occupational Safety and Health Program, FAA Order 1050.1E, Environmental Impacts: Policies and Procedures, etc.). The FAA Acquisition System Toolset (FAST) provides policy and guidance in order to ensure that EOSH regulations are considered in the acquisition process. The EOSH policy is as follows:

FAA investment programs shall comply with relevant federal, state, and local regulations, and FAA orders, specifications, and standards pertaining to environmental and occupational safety and health (EOSH) requirements, and energy and water requirements. FAA lines of business and staff offices must comply with all applicable requirements of the National Environmental Policy Act (NEPA) in accordance with the current version of FAA Order 1050.1, Environmental Impacts: Policies and Procedures. Service organizations responsible for implementing investment programs must consider EOSH and energy and water requirements, and address them throughout the lifecycle management process in order to:

- *Ensure the installation and operation of systems, equipment, facilities, and related program activities will not adversely impact personnel safety and health or the environment; and*
- *Ensure the acquisition program baseline of the investment initiative reflects the schedule and cost of EOSH requirements.*

Questions on the applicability of state and local EOSH requirements to federal acquisitions should be referred to the Office of the Chief Counsel for an evaluation of the supremacy clause and sovereign immunity implications.

The following examples illustrate some of the requirements:

- **Clean Air Act (CAA)**: The CAA established a comprehensive program for protecting and enhancing the nation's air quality and stratospheric ozone layer. State air pollution prevention agencies have developed emission control strategies and permit programs, particularly for new construction or modifications of sources of air pollution. The CAA also established the National Emission Standards for Hazardous Air Pollutants (NESHAP) requiring permitting and implementation of pollution control standards for certain air pollutants.
- **Clean Water Act (CWA)**: The CWA established the National Pollutant Discharge Elimination System (NPDES), which controls water pollution by regulating point sources that discharge pollutants into the waters of the United States. At ATO facilities, cooling tower discharges, boiler blow-down and/or other thermal discharges to waters of the United States may require an NPDES permit. Additionally, storm water discharges resulting from ATO construction activities may require an NPDES permit.
- **Protection of Cultural Resources**: ATO installs and maintains thousands of NAS facilities across the United States and therefore must consider the impact these installations could have on culturally significant sites. Cultural resources include, but are not limited to historic properties (as listed in or eligible for the National Register of Historic

Places), Native American graves and cultural items, and archeological sites. Cultural resource management refers to the legally mandated protection of these resources.

- **National Environmental Policy Act (NEPA)**: NEPA "requires preparation of an environmental assessment or an environmental impact statement for all proposed federal actions that are not categorically excluded. Depending on the results, an environmental assessment can lead to an environmental impact statement or a finding of no significant impact. Following the prescribed review periods, FAA may make a decision on the federal action."
- **Occupational Safety and Health Requirements**: The Occupational Safety and Health Administration (OSHA) "requires a safe and healthful workplace for all employees, and compliance with OSHA standards."

  For example: OSHA (29 CFR §1910.38) and GSA (Federal Property Management Regulations) require the FAA to establish and maintain an Occupant Emergency Plan for all FAA facilities. In the event an acquisition program impacts egress routes or fire safety of a facility, the plan must be updated by the program office or the Product Team performing the project.
- **Sustainability Requirements**: The Energy Policy Act of 2005, the Energy Independence and Security Act of 2007, and related Executive Orders (Executive Order 13423, Strengthening Federal Environmental, Energy, and Transportation Management, and Executive Order 13514, Federal Leadership in Environmental, Energy, and Economic Performance) established energy conservation and efficiency, water conservation and efficiency, and storm water management requirements for the federal government. They require federal agencies to measure, report, and reduce greenhouse gas emissions from direct and indirect activities, and eliminate waste, recycle, and prevent pollution. Additionally, the Guiding Principles for Federal Leadership in High Performance and Sustainable Buildings commits FAA to a common set of sustainable principles for integrated design, energy performance, and water conservation at occupied and unoccupied FAA facilities that support essential systems.
- **Hazardous Waste Management Requirements**: The Resource Conservation and Recovery Act (RCRA) is the primary federal statute regulating the management and disposal of hazardous wastes. ATO facilities must manage hazardous wastes in accordance with the requirements of both federal and state-specific programs to ensure compliance and proper management of the wastes. FAA is exposed to "cradle to grave" liability for hazardous wastes. Proper management and disposal will minimize the agency's exposure to this liability.

Environmental, occupational safety and health, and sustainability considerations apply from the beginning of the lifecycle management process through product disposal. The acquisition program baseline shall incorporate estimates for the full cost of complying and allow sufficient time for doing so. FAST contains procedural guidance for required actions.

When applied early, HMM/EE and EOSH processes identify applicable requirements to include in the development and acquisition of new systems, thereby providing significant savings through risk mitigation, cost avoidance, and enhancement of system efficiency. For example, a program fielding a new system would want to consider how the equipment will be maintained, and whether personnel will be exposed to any hazards when they perform maintenance activities. They can then evaluate options for eliminating the hazard, or controlling the hazard to an acceptable level of risk, and incorporate associated costs into the program baseline. Product specifications must, wherever possible and appropriate, require the use of sustainable products, including environmentally preferable, energy and water efficient, recycled content, non-ozone depleting, less or non-toxic, and USDA-designated bio-based products. For example, when preparing specifications and purchase descriptions for supplies and services, they must ensure that each comply with the Clean Air Act and substitute safe alternatives to ozone depleting substances, as approved by EPA’s Significant New Alternatives Policy (SNAP) program. Additionally, consideration of environmental impacts on systems while they are in the developmental stages ensures their functionality in various field conditions.

When applied as part of in-service program management, HMM/EE and EOSH processes analyze the impact that engineering changes in the field may have on environmental concerns. Additionally, HMM/EE and EOSH processes evaluate the impact that EOSH regulatory changes may have on currently fielded systems.

At the end of the program lifecycle, HMM/EE and EOSH processes ensure compliance with applicable requirements during decommissioning and disposition. As obsolete equipment is removed, employment of HMM/EE and EOSH processes can ensure that replacement equipment complies with applicable EOSH regulations and sustainability requirements. Further, decommissioning and removal of obsolete equipment require use of HMM/EE and EOSH to ensure that final disposition/disposal of obsolete equipment are conducted in accordance with applicable environmental requirements.

Programs that fail to fully incorporate HMM/EE and EOSH principles may have significant impacts on NAS operations. Noncompliant programs may:

- Risk having equipment removed from service through regulatory enforcement actions;
- Require costly post-fielding/retrofit modifications; or
- Incur fines for noncompliance with mandated requirements.

Additionally, costs associated with new equipment fielding, and obsolete equipment disposition and disposal may lead to significant budgeting issues if they are not considered during the program development phase.

5.7.2 HMM/EE and EOSH Outputs

Throughout the various phases of the system acquisition process, HMM/EE and EOSH principles are applied in developing and reviewing key documents. Early implementation of these principles minimizes the impact that EOSH and sustainability requirements may have on system costs and operations. During the preliminary activities, such as development of mission needs, requirements, and investment analysis, HMM/EE and EOSH are used to make initial assumptions and estimates on how EOSH and sustainability considerations may come into play throughout the various lifecycle stages. HMM/EE and EOSH activities during this phase may include:

- Identifying EOSH and sustainability requirements associated with the various program alternatives, and then tailoring requirements to the selected alternative; and
- Incorporating EOSH and sustainability requirements into the program requirements document, Business Case Analysis Report (BCAR), and Implementation Strategy and Planning Document (ISPD).

During the solution implementation phase of the acquisition process, HMM/EE and EOSH processes are used to:

- Shape portions of the statement of work (SOW) and system specification documents as they relate to EOSH and sustainability considerations (for example, SOWs may be developed to support FAA efforts to meet National Environmental Policy Act requirements that federal agencies consider environmental impacts as part of proposed federal actions for federal building energy efficiency performance standards); and
- Incorporate EOSH and sustainability requirements into system designs and implementation plans.

During the in-service management phase of the system lifecycle, HMM/EE and EOSH are used to address issues that may arise unexpectedly in the field. In particular, older pieces of equipment that may not have been developed with HMM/EE, EOSH, and sustainability in mind may require corrective measures to meet current regulations. Additionally, ever-changing regulations may impact the way systems are operated. Finally, as old systems are decommissioned, HMM/EE and EOSH are necessary to ensure that all disposal actions consider applicable environmental laws.

Figure 71 shows the key activities in the acquisition life cycle where EOSH and sustainability requirements are considered and incorporated into various program artifacts.

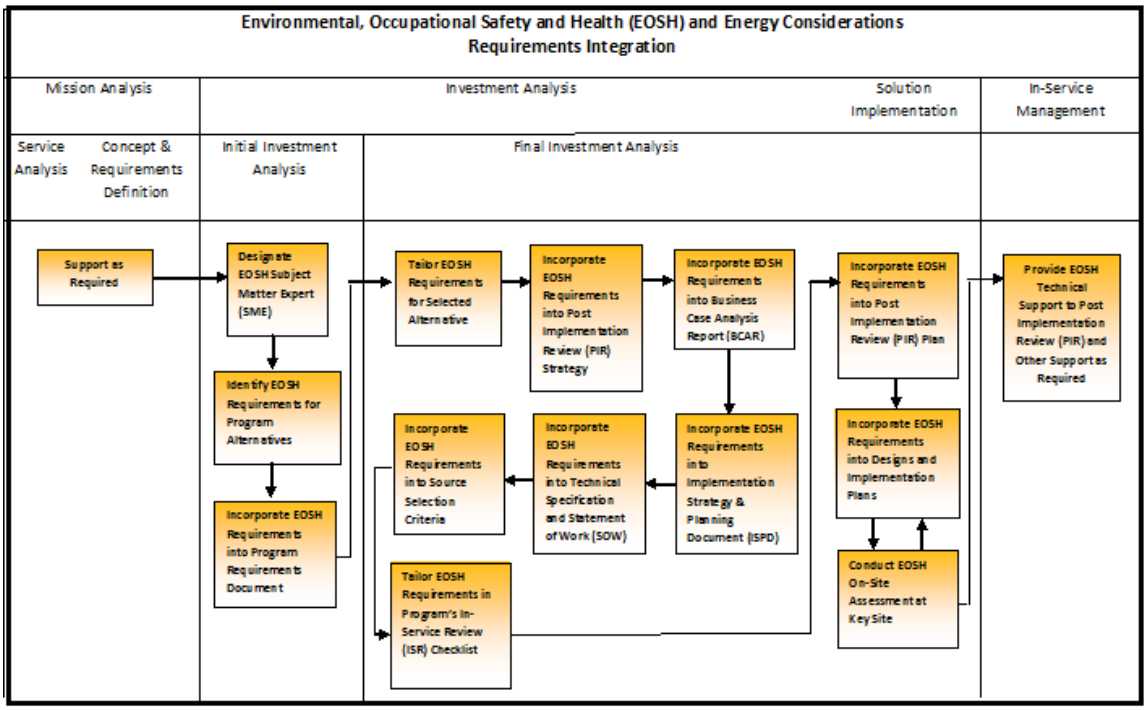


Figure 71: EOSH Requirements Integration in AMS Life Cycle

Program Integration

As part of the SE process, HMM/EE and EOSH provide expertise for developing various documents required for program integration. Throughout the various lifecycle phases, HMM/EE and EOSH processes ensure that all applicable EOSH and sustainability regulations and environmental conditions are properly addressed so that their impacts are addressed appropriately. For example, HMM/EE and EOSH processes would support development of the IRD, keeping in mind environmental regulations that require federal agencies to verify that their activities do not negatively impact certain ecosystems. Similarly, HMM/EE and EOSH's role in developing Integrated Program Plans, SOWs, Reutilization and Disposition Plans, and other such documents generates comments and input concerning compliance requirements. The compliance requirements may impact the progress of program implementation, and FAA's compliance status and future liabilities.

Included in the HMM/EE and EOSH aspects of program integration is a functional analysis of the OSED (see Chapter 12, Functional and Performance Allocation). This portion of the functional analysis ensures that the environmental conditions that the various systems face are fully considered and that plans are appropriately developed to address identified conditions. Figure 72 depicts HMM/EE and EOSH inputs and outputs.

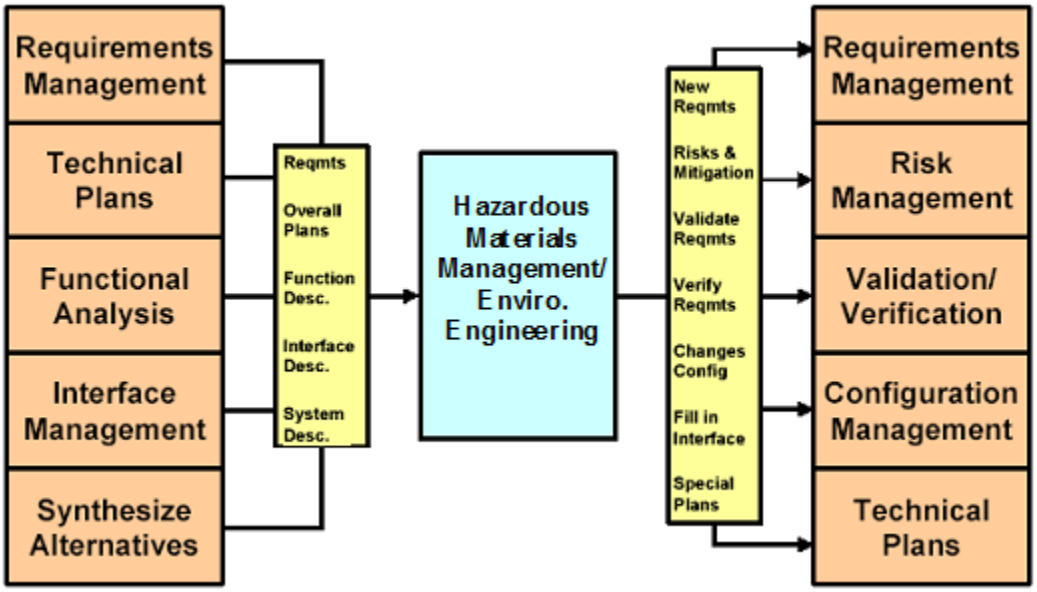


Figure 72: HMM/EE Relationship to Other Systems Engineering Processes

Program Planning

FAA Order 1050.17, Airway Facilities Environmental Compliance Program, implements the overall program for environmental compliance at FAA facilities. Each region in the agency has an Environmental Compliance Plan (ECP). The ECP is designed to identify and address compliance requirements in 19 environmental areas for all facilities, and therefore all systems within a region.

In addition, FAA Order 4600.27B, Personal Property Management, and AMS Section 2.7, In-Service Management, provide the requirements and framework for developing and implementing system-specific disposal plans for obsolete systems. These disposal plans are part of the Integrated Program Plan appendices; see Chapter 3, Integrated Technical Planning Process.

Products

Additionally, the HMM/EE and EOSH processes must provide a program with the capability to produce an inventory of hazardous materials that fielded equipment may contain. This information has many purposes, including, but not limited to:

- Ensuring protection of the environment and surrounding communities;
- Ensuring regulatory compliance during the program's operational life;
- Supporting the safety of personnel working with equipment; and
- Supporting disposal efforts when obsolete equipment is removed from service.

Additional Information

For sources of information used to generate content throughout this section, see References.

6 References

6.1 Reference Sources

These references represent in-text citations and r overall sources of information used to generate content throughout each listed manual section. Duplicate references are identified by their reference codes; for full citation information, refer to the first mention of the reference code in the table below.

Reference Code	Reference Source
1.4 Plan, Do, Check, Act	
Anderson 2011	Anderson, Chris. How Are PDCA Cycles Used?, *Bizmanualz*, June 7, 2011. http://www.bizmanualz.com/blog/how-are-pdca-cycles-used-inside-iso-9001.html
1.5 System of Systems	
Maier 1998	Maier, Mark W. 1998. “Architecting Principles for System-of-systems.” Systems Engineering 1 (4): 267–284.
Carlock 2001	Carlock, Paul G, and Robert E Fenton. 2001. “System of Systems (SoS) Enterprise Systems Engineering for Information-intensive Organizations.” Systems Engineering 4 (4): 242–261.
3.1 Operational Concept Development	
Blanchard 1999	Blanchard, Benjamin S, and Wolter J Fabrycky. 1998. *Systems Engineering and Analysis*. 3rd ed. Upper Saddle River, NJ: Prentice-Hall Inc.
CMMI-DEV 2006	*CMMI for Development, Version 1.2*. Standard. Pittsburgh, PA: Carnegie Mellon University/Software Engineering Institute. 2006.
EIA-632 1999	*Processes for Engineering a System*. Standard. Arlington, VA: Government Electronics and Information Technology Association. 1999.
IEEE 1220 2005	*IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers. 2005.
IEEE 1362 1998	*IEEE Guide for Information Technology - System Definition - Concept of Operations (ConOps) Document*. Standard. New York: The Institute of Electrical and Electronics Engineers. December 31, 1998.
INCOSE 2010	*INCOSE Systems Engineering Handbook: A Guide for System Lifecycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering. 2010.
ISO-15288 2008	*Systems Engineering: System Lifecycle Processes*. Standard. Geneva, Switzerland: International Organization for Standardization. 2008.
NASA 2007	*NASA Systems Engineering Handbook*. Handbook. Washington, DC: National Aeronautics and Space Administration, December. 2007.
3.2 Functional Analysis	

Reference Code	Reference Source
Blanchard 1999 CMMI-DEV 2006 EIA-632 1999 IEEE 1220 2005 IEEE 1362 1998 INCOSE 2010 ISO-15288 2008	*Previously cited.*
Beude 2000	Buede, Dennis M. 2000. *The Engineering Design of Systems: Models and Methods*. New York: John Wiley & Sons.
Grady 2006	Grady, Jeffrey O. 2006. *System Requirements Analysis*. Burlington, MA: Elsevier Inc.
IEEE 830 1998	*IEEE Recommended Practice for Software Requirements Specifications*. Standard. New York: IEEE Computer Society. October 20, 1998.
IEEE 1223 1998	*IEEE Guide for Developing System Requirements Specifications*. Standard. New York: IEEE Computer Society. December 8, 1998.
3.3 Requirements Analysis	
EIA-632 1999 IEEE 1220 2005 INCOSE 2010 ISO-15288 2008 NASA 2007	*Previously cited.*
DAU 2001	*Systems Engineering Fundamentals*. Fort Belvoir, VA: Defense Acquisition University Press. January 2001.
DAU 2010	*Defense Guidebook*. Fort Belvoir, VA: Department of Defense, December 22, 2010. https://dag.dau.mil/Pages/Default.aspx
FAA AMS 2012	*FAA AMS Lifecycle Verification and Validation Guidelines, Ver 2.0*. Atlantic City International Airport, NJ: William J Hughes Technical Center. Federal Aviation Administration. 2012.
3.4 Architectural Design Synthesis	
EIA-632 1999 IEEE 1220 2005 INCOSE 2010 ISO-15288 2008	*Previously cited.*
3.5 Cross Cutting Technical Methods	

Reference Code	Reference Source
IEEE 1220 2005 INCOSE 2010 ISO-15288 2008 FAA AMS 2012 NASA 2007	*Previously cited.*
ATO-S 2008	ATO-S 2008-12 Version 1.5, 2008, Safety Risk Management Guidance for System Acquisitions (SRMGSA), Management System (SMS) and Acquisition Management System (AMS) Guidance Document, December.
Lankhorst 2009	Lankhorst, Marc, *Enterprise Architecture at Work*, Springer, 2009, page 122
4.1 Integrated Technical Management	
Blanchard 1998 DAU 2001 DAU 2010 EIA-632 1999 IEEE 1220 2005 INCOSE 2010 ISO-15288 2008 NASA 2007	*Previously cited.*
Sage 2000	Sage, Andrew P, and James E Armstrong Jr. 2000. *Introduction to Systems Engineering*. Wiley Series in Systems Engineering. New York: John Wiley & Sons.
4.2 Interface Management	
IEEE 1220 2005 INCOSE 2010 NASA 2007	*Previously cited.*
4.3 Risk Management	
IEEE 1220 2005 INCOSE 2010 ISO-15288 2008 NASA 2007	*Previously cited.*
FAA FAST	FAA Acquisition System Toolset (FAST). Washington, DC: U.S. Department of Transportation, Federal Aviation Administration. http://fast.faa.gov/
4.4 Configuration Management	

Reference Code	Reference Source
IEEE 1220 2005 INCOSE 2010 ISO-15288 2008 NASA 2007	*Previously cited.*
4.5 Systems Engineering Information Management	
IEEE 1220 2005 INCOSE 2010 NASA 2007	*Previously cited.*
4.6 Decision Analysis	
IEEE 1220 2005 INCOSE 2010 NASA 2007	*Previously cited.*
4.7 Verification and Validation Process	
CMMI-DEV 2006 EIA-632 1999 IEEE 1220 2005 INCOSE 2010 ISO-15288 2008	*Previously cited.*
FAA AMS 2012	*FAA AMS Lifecycle Verification and Validation Guidelines, Ver 2.0*. Atlantic City International Airport, NJ: William J Hughes Technical Center. Federal Aviation Administration. 2012.
IREB 2012	"International Requirements Engineering Board," 2012 http://www.certified-re.de/en/
5.1 Reliability, Maintainability, and Availability	
ENG TOOLKIT 1993	*Reliability Engineer's Toolkit. R*ome Laboratory. Griffiss Air Force Base, April 1993.
FAA RMA 2008	*FAA Reliability, Maintainability and Availability (RMA) Handbook*, FAA-HDBK-006A, January 7, 2008.
FAA SYS SAFETY 2000	*System Safety Handbook. F*ederal Aviation Administration, 30 September 2000.
SAFETY ARP4761 1996	*Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. A*erospace Recommended Practice, ARP4761. Society of Automotive Engineers, Inc. Issued 1996-12.
SOFTWARE 89-97714 1989	*Guide to the Assessment of Reliability of Systems Containing Software. D*ocument No. 89/97714. British Standards Institution, 12 September 1989.
5.2 Lifecycle Engineering	

Reference Code	Reference Source
DOD MIL-PRF-49506 1996	*Logistics Management Information.* MIL-PRF-49506. Washington, DC: U.S. Department of Defense, 11 November 1996.
FAA COTS 2010	FAA COTS Risk Mitigation Guide / Practical Methods for Effective Acquisition and Support, V 3.2 dated 1/2010 http://fast.faa.gov/syseng/index.htm
FAA FAST	*Previously cited.*
FAA ILSPG 2001	*Integrated Logistics Support Process Guide (ILSPG). W*ashington, DC: U.S. Department of Transportation, Federal Aviation Administration, June 2001. http://fast.faa.gov/toolsets/ILSPG/
FAA Order 4800.2C 1996	*Utilization and Disposal of Excess and Surplus Personal Property*. Order 4800.2C. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, 31 May 1996.
FAA Order 6000.30C 2001	*National Airspace System Maintenance Policy*. Order 6000.30C. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, 25 January 2001.
Jones 1998	Jones, James V. I*ntegrated Logistics Support Handbook*. Second Edition. Special Reprint Edition. New York, NY: McGraw-Hill Professional Book Group, 1998. ISBN: 0070331391.
5.3 Electromagnetic Environmental Effects and Spectrum Management	
DOD MIL-STD-461F 2007	"Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," MIL-STD-461F, U.S. Department of Defense, Washington, DC, 10 Dec 2007. https://assist.daps.dla.mil/docimages/A/0000/0003/5789/000000607244_000000207288_WAQUATEUOJ.PDF?CFID=39736049&CFTOKEN=90270861&jsessionid=5c30aae09cb9a4345b011a5a2c68214b6b6a
DOT Order 5240.3	"Radio Frequency Spectrum Use," DOT Order 5420.3, U.S. Department of Transportation, Washington, DC.
FAA G-2100H 2005	"Electronic Equipment, General Requirements," Section 3.3.2 "Electromagnetic Compatibility" FAA-G-2100H, U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 9 May 2005
FAA Order 6050.19E 2000	"Radio Spectrum Planning," FAA Order 6050.19E, U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 30 June 2000. http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/spec_management/library/view/documents/rfi/RFI_6050_19e.pdf
FAA Order 6050.32B 2005	"Spectrum Management Regulations and Procedures Manual," FAA Order 6050.32B, U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 17 November 2005. http://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/73412

Reference Code	Reference Source
FAA SPECTRUM 2002	"Radio Spectrum Plan 2001-2010 (2002 Revision)", U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 30 September 2002. http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/spec_management/library/view/documents/RSP_2002.pdf
IEEE 149 1977	"IEEE Standard Test Procedures for Antennas," IEEE Std-149-1977, Institute of Electrical and Electronics Engineers, New York, NY. (Reaffirmed in 2003), ISBN 1-5593-7609-0. http://standards.ieee.org/findstds/standard/149-1977.html
IEEE C63.5 1998	"American National Standards for Electromagnetic Compatibility - Radiated Emission Measurements in Electromagnetic Interference (EMI) Control-Calibration of Antennas (9 kHz to 40 GHz)," IEEE C63.5-1998, Institute of Electrical and Electronics Engineers, New York, NY. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=741969
NTIA 2011	"Manual of Regulations and Procedures for Federal Radio Frequency Management (May 2011 Revision of the 2008 Edition)," U.S. Department of Commerce, National Telecommunications and Information Administration, Washington, DC. 2011. http://www.ntia.doc.gov/page/2011/manual-regulations-and-procedures-federal-radio-frequency-management-redbook
RTCA 1997	"Environmental Conditions and Test Procedures for Airborne Equipment," (With Three Changes Issued), RTCA/DO-160F, RTCA, Inc., Washington, DC. http://www.rtca.org/digest_nm/181-FEB08Frontpage.pdf
SAE ARP958 1999	"Electromagnetic Interference Measurement Antennas; Standard Calibration Method," ARP958, revision D, SAE International, Warrendale, PA, March. 1999 http://standards.sae.org/wip/arp958d
5.4 Human Factors Engineering	
Ahlstrom 2011	Ahlstrom, V. & Longo, K. *Human Factors Design Standard. D*ocument HF-STD-001. Atlantic City International Airport, NJ: Federal Aviation Administration William J. Hughes Technical Center, February 2011. (http://hf.tc.faa.gov/hfds/)
Boff 1988	Boff, K., and Lincoln J., eds. E*ngineering Data Compendium: Human Perception and Performance. V*ols. *1-3. W*right-Patterson Air Force Base, OH: Harry G. Armstrong Aerospace Medical Research Laboratory, 1988.
Booher 2003	Booher, H. R., ed. Handbook of Human Systems Integration, New York, NY: John Wiley & Sons, Inc., 2003.
Booher 1990	Booher, H. R., ed. MANPRINT: An Approach to Systems Integration, New York, NY: Van Nostrand Reinhold, 1990.
Chapanis 1996	Chapanis, Alphonse. Human Factors in Systems Engineering, John Wiley and Sons, Inc., 1996.
FAA HF ACQ 2003	*FAA Human Factors Acquisition Job Aid*. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, December 2003. http://www.hf.faa.gov/docs/508/docs/jobaid.pdf

Reference Code	Reference Source
FAA HF INTEGRATION 2004	*FAA Human Factors Integration Guide for Mission and Service Area Analysis.* Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, September 2004.
FAA HF INVEST 2006	*FAA Human Factors Assessments in Investment Analysis: Definition and Process Summary for Cost, Risk, and Benefit, v. 1.4b.* Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, June 2006
FAA HF REQ 2011	*FAA Guidelines for Human Factors Requirements Development.* Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, June 2011.
FAA HF-STD-004 2009	*FAA Requirements for Human Factors Program.* Document HF-STD-004. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, June 2009.
FAA Order 9550.8 1993	*FAA Human Factors Policy. F*AA Order 9550.8. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, October 1993.
Hendrick 2001	Hendrick, Hal W. and Kleiner, Brian M, *Macroergonomics: An Introduction to Work System Design*, 2001.
Meister 1985	Meister, D. *Behavioral Analysis and Measurement Methods*. New York, NY: John Wiley & Sons, Inc., 1985.
MIL-HDBK01908B 1999	*Definitions of Human Factors Terms*. MIL-HDBK-1908B, August 1999.
Wickens 1997	Wickens, C., Mavor, A., and McGee, J., eds. *Flight to the Future: Human Factors in Air Traffic Control*. Washington, DC: National Academy Press, 1997.
Wickens 1998	Wickens, C., Mavor, A., Parasuraman, R., and McGee, J., eds. *The Future of Air Traffic Control: Human Operators and Automation*. Washington, DC: National Academy Press, 1998.
5.5 Information Security Engineering	
CLINGER 1996	Clinger-Cohen Act of 1996.
FAA Order 1370.82	FAA Order 1370.82, *Information Systems Security Program.*
FIPS PUB 199	*Standards for Security Categorization of Federal Information and Information Systems.*
FIPS PUB 200	*Minimum Security Requirements for Federal Information and Information Systems.*
FISMA 2002	Federal Information Security Management Act (FISMA) of 2002.
NIST 800-18	NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems.*
NIST 800-27	NIST Special Publication 800-27 Rev. A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security).*
NIST 800-30	NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems.

Reference Code	Reference Source
NIST 800-37	NIST Special Publication 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems.*
NIST 800-55	NIST Special Publication 800-55, *Performance Measurement Guide for Information Security.*
NIST 800-57	NIST Special Publication 800-57, *Guide for Assessing the Security Controls in Federal Information Systems.*
OMB CIRC A-130	*OMB Circular A-130, Management of Federal Information Resources.*
5.7 Hazardous Materials Management / Environmental Engineering	
EISA 2007	Energy Independence and Security Act of 2007
EPA 2005	Energy Policy Act of 2005.
Exec Order 13423	*Executive Order 13423, Strengthening Federal Environmental, Energy, and Transportation Management.*
Exec Order 13514	*Executive Order 13514, Federal Leadership in Environmental, Energy, and Economic Performance.*
FAA FAST 2.7	*In-Service Management.* FAA Acquisition Management System, Section 2.7. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC. http://fast.faa.gov.
FAA Order 1050.10C	*Prevention, Control, and Abatement of Environmental Pollution at FAA Facilities.* FAA Order 1050.10C. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.
FAA Order 1050.17	Airway Facilities Environmental and Safety Compliance Program. FAA Order 1050.17. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.
FAA Order 1053.1A	*Energy and Water Management Program for FAA Buildings and Facilities*. FAA Order 1053.1A. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.
FAA Order 4600.27B	*Personal Property Management*. FAA Order 4600.27B. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.
FAA Order 5050.4B	*National Environmental Policy Act (NEPA) Implementing Instructions for Airport Projects*. FAA Order 5050.4B. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.
OSHA 1970	Occupational Safety and Health Act of 1970, and the implementing regulations at 29 CFR 1910, 29 CFR 1926 and 29 CFR 1960.

6.2 Additional Tools and Reading Recommendations

The below references, tools, and websites serve as additional information sources for readers interested in learning more about specific manual topics.

Reference or Tool	Brief explanation
2.2 Phases of the AMS Lifecycle Management Process	
Joint Planning and Development Office (JPDO) *Concept of Operations*	http://www.jpdo.gov/library/NextGen_v2.0.pdf The JPDO ConOps provides an operational view of NextGen and how it will operate in 2025 and beyond. It includes the role of every air transportation stakeholder (NASA, DoD, DOT, DHS, etc). This document should be used as a reference to understand the long-term impact of capabilities on the overall management of air traffic.
Radio Technical Commission for Aeronautics (RTCA) *NextGen Mid-Term Implementation Task Force Report*	http://www.faa.gov/about/initiatives/nextgen/media/nextgen_progress_report.pdf The RTCA task force report was created to forge community-wide consensus on the recommended NextGen operational improvements to be implemented during the transition between now and 2018. The task force looked for opportunities to accelerate the transition to technologies defined in the NextGen implementation plan. This document should be used as a reference to understand the specific strategies for accelerating certain types of technology.
Federal Aviation Administration (2010) *National Aviation Research Plan*	http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/nextgen/research_tech_dev/research_planning/narp/media/pdf/NARP_2010.pdf The NARP establishes the research and development programs for FAA. Published annually, the NARP bridges the near-term goals of the FAA Flight Plan (2009-2013) with the mid-term goals of the NextGen Implementation Plan (2012-2018) and the far-term goals of the JPDO's Integrated Work Plan (2015-2025). The NARP can be used to understand the impact a specific technology has on the goals of the agency in the near, mid, and far term.
Federal Aviation Administration (2010) *NextGen Implementation Plan*	https://intranet.faa.gov/faaemployees/org/linebusiness/ato/operations/technical_operations/ajw1/ajw14/media/NextGen%20Implementation%20Plan%202010.pdf The NextGen Implementation Plan provides an overview of the FAA's ongoing transition to NextGen. The plan lays out the agency's vision between now and the mid-term time frame (2012-2018). The plan identifies the goals for technology and program deployment. This document should be used to tie specific program shortfalls to the goals of NextGen.
Federal Aviation Administration (2009-2013) *FAA Flight Plan* (to be replaced by FAA Destination 2025)	http://www.faa.gov/about/plans_reports/media/flight_plan_2009-2013.pdf The Flight Plan contains the five-year strategic plan for FAA from 2009 through 2013. FAA is currently developing a replacement for the Flight Plan called "Destination 2025." This document should be used to tie specific program shortfalls to the strategic goals of the agency. There should be a direct link between a strategic goal for improvement and the shortfall identified during service-level analysis.

Reference or Tool	Brief explanation
Federal Aviation Administration (2010) *Investment Decision Authority (IDA) Process Guidance*	https://intranet.faa.gov/faaemployees/org/linebusiness/ato/acquisition_business/ipm/media/file/Preparing%20for%20a%20JRC/IDAGuidance%208_13_2010.pdf This document is supplemental to the information in AMS policy. It explains the types of decisions and prerequisite actions, roles and responsibilities, and procedures required to receive an investment decision from an agency investment decision authority. This document should be used to reference all items that must be completed prior to a Concept and Requirements Definition (CRD) Readiness Decision.
Federal Aviation Administration. (2011) *Acquisition Management System Policy*	http://fasteditapp.faa.gov/ams/do_action?do_action=ListTOC&contentUID=4 AMS Policy establishes all requirements for acquisition management at FAA. Specifically, it contains service analysis and CRD requirements for the activities that must be completed, the outputs and products of each activity, who is responsible for each activity, and who approves each output.
Federal Aviation Administration (2006) *National Airspace System, System Engineering Manual* (Version 3.1)	http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/operations/sysengsaf/seman/ This previous version of this document provides a framework for implementing systems engineering across FAA. The document does not mandate any formal practice but acts as a reference for conducting specific systems engineering activities.
Federal Aviation Administration (2007) *National Airspace System Enterprise Architecture Framework (NASEAF), Volume III: Product Implementation Methodologies* (Version 2.00)	https://nasea.faa.gov/file/get/814 This document describes the Air Traffic Organization's method for building architectures. It defines and describes the products and processes that apply to architecture development for all levels (enterprise, service-unit, and project). This document can be used to understand the NAS EA framework and its structure. It should be referenced during the construction of project-level architecture products and amendments.
Federal Aviation Administration (2010) *Service Analysis and Concept and Requirements Definition Guidelines*, (Version 4.0)	http://fast.faa.gov/mission/conc_req_def.htm This document describes "how-to" guidance for moving through the service analysis and CRD phases of AMS. The document includes specific information such as templates, process instructions, required reviewing organizations, and required signature authorities. This document in addition to AMS policy should be used to understand the AMS requirements for service analysis and CRD.
2.2.3 Concept and Requirements Definition	
FAA Acquisition Management System Toolset (FAST)	http://fast.faa.gov See sections on CRD policy , CRD readiness decision policy, an IARD policy.
NAS Enterprise Architecture Framework (NASEAF)	https://nasea.faa.gov/file/get/814 Paragraph 4.1.1 defines the architectural products required during CRD.

Reference or Tool	Brief explanation
NAS Requirements Document NAS-RD-2012	These enterprise level requirements establish the top level of a much more detailed requirements database development effort in support of NextGen development and technical management.
2.2.4 Investment Analysis	
Federal Aviation Administration (2006) *National Airspace System, System Engineering Manual* (Version 3.1)	http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/operations/sysengsaf/seman/ See sections on Requirements Management, Functional Analysis, Trade Studies, Specialty Engineering, Risk Management, and Validation and Verification.
FAA Acquisition Management System Toolset (FAST)	http://fast.faa.gov See sections on Investment Analysis Standard Guidance , Investment Analysis Process Guidance, and Business Case Analysis Guidance and Template.
NAS Enterprise Architecture Framework (NASEAF)	https://nasea.faa.gov/file/get/814
FAA Investment Planning & Analysis Website	http://www.ipa.faa.gov See sections on: Investment Analysis Processes and Products; Building the Business Case; Methodologies: Cost Analysis, Benefits Analysis, Economic Analysis, Risk Analysis, Schedule Analysis; Communicating Your Business Case; Evaluating the Business Case; Business Case Guidelines and Templates; Guidelines for Conducting Shortfall Analysis; Guidelines for Defining and Applying the Legacy Case; Investment Analysis Plan Guidelines and Template; Guidelines for Defining and Determining the Required Service Period, Economic Service Life, and Analysis Period; Guidelines for FAA Cost Estimating; Guidelines for Documenting Cost Basis of Estimate; Guidelines for Benefits Estimating and Report Template; Guidelines for Conducting Investment Analysis Risk Assessment; AJF Business Case Evaluation and Assessment Guideline.
2.2.5 Solution Implementation	
FAA Acquisition Management System Toolset (FAST) Acquisition Management Policy Section 2.5 Solution Implementation	http://fast.faa.gov AMS Policy establishes all requirements for acquisition management over the full lifecycle at FAA. Specifically, it specifies requirements for the activities that must be completed during solution implementation, the outputs and products of each activity, the responsible agent or agents, and who approves each output.
FAA AMS Lifecycle Verification and Validation Guidelines	This document guides the application of verification and validation policies across FAA. It defines terminology and illustrates how to accomplish verification and validation and in each phase of the AMS Lifecycle.
NextGen and Operations Planning Services, Test and Evaluation Handbook, document number VVSPT-A2-PDD-013	This document provides detailed guidance as to how to conduct Test and Evaluation for NAS-related systems.

Reference or Tool	Brief explanation
Solution Implementation Acquisition Practices Toolkit	https://employees.faa.gov/org/linebusiness/ato/operations/technical_operations/best_practices/Lifecycle/solution_implementation/ This toolkit contains processes, flowcharts, activities, checklists, good examples of works products, and other tools helpful to service team members executing solution implementation.
2.2.6 In-Service Management	
FAA Acquisition Management System Toolset (FAST)	http://fast.faa.gov AMS Policy establishes all requirements for acquisition management over the full lifecycle at FAA. Specifically, it lists requirements for the activities that must be completed during in-service management, the outputs and products of each activity, the responsible agent or agents, and who approves each output.
3.1 Operational Concept Development	
INCOSE Systems Engineering Handbook: A Guide for System Lifecycle Processes and Activities	Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering Depicts a similar process as Operational Concept
The Official OMG SysML site OMG Systems Modeling Language	http://www.omgsysml.org (Accessed September 7, 2012) See specifications and tutorials.
Writing Better Requirements	Alexander, Ian F, and Richard Stevens. 2002. *Writing Better Requirements*. New York: Addison-Wesley.
The Engineering Design of Systems: Models and Methods	Buede, Dennis M. 2000. *The Engineering Design of Systems: Models and Methods*. New York: John Wiley & Sons.
Systems Engineering and Analysis	Blanchard, Benjamin S, and Wolter J Fabrycky. 1998. *Systems Engineering and Analysis*. 3rd ed. Upper Saddle River, NJ: Prentice-Hall Inc.
System Requirements Analysis	Grady, Jeffrey O. 2006. *System Requirements Analysis*. Burlington, MA: Elsevier Inc.
Introduction to Systems Engineering	Sage, Andrew P, and James E Armstrong Jr. 2000. *Introduction to Systems Engineering*. Wiley Series in Systems Engineering. New York: John Wiley & Sons.
Handbook of Systems Engineering and Management	Sage, Andrew P, and William B. Rouse (eds). 2009. *Handbook of Systems Engineering and Management*, 2nd ed. Wiley Series in Systems Engineering. New York: John Wiley & Sons.
Systems Practices as Common Sense	Sobkiw, Walter. 2011. *Systems Practices as Common Sense*. Cherry Hill, NJ: CassBeth
3.2 Functional Analysis	
INCOSE Systems Engineering Handbook: A Guide for System Lifecycle Processes and Activities	Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering Depicts a similar process as Functional Analysis Process

Reference or Tool	Brief explanation
Writing Better Requirement	Alexander, Ian F, and Richard Stevens. 2002. *Writing Better Requirements*. New York: Addison-Wesley.
The Engineering Design of Systems: Models and Methods	Buede, Dennis M. 2000. *The Engineering Design of Systems: Models and Methods*. New York: John Wiley & Sons.
Systems Engineering and Analysis	Blanchard, Benjamin S, and Wolter J Fabrycky. 1998. *Systems Engineering and Analysis*. 3rd ed. Upper Saddle River, NJ: Prentice-Hall Inc.
System Requirements Analysis	Grady, Jeffrey O. 2006. *System Requirements Analysis*. Burlington, MA: Elsevier Inc.
Introduction to Systems Engineering	Sage, Andrew P, and James E Armstrong Jr. 2000. *Introduction to Systems Engineering*. Wiley Series in Systems Engineering. New York: John Wiley & Sons.
Handbook of Systems Engineering and Management	Sage, Andrew P, and William B. Rouse (eds). 2009. *Handbook of Systems Engineering and Management*, 2nd ed. Wiley Series in Systems Engineering. New York: John Wiley & Sons.
Practices as Common Sense	Sobkiw, Walter. 2011. *Systems Practices as Common Sense*. Cherry Hill, NJ: CassBeth
3.4 Architectural Design Synthesis	
INCOSE Systems Engineering Handbook: A Guide for System Lifecycle Processes and Activities	Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering Depicts a similar process as Design Synthesis Process
The Engineering Design of Systems: Models and Methods	Buede, Dennis M. 2000. *The Engineering Design of Systems: Models and Methods*. New York: John Wiley & Sons.
Systems Engineering and Analysis	Blanchard, Benjamin S, and Wolter J Fabrycky. 1998. *Systems Engineering and Analysis*. 3rd ed. Upper Saddle River, NJ: Prentice-Hall Inc.
System Requirements Analysis	Grady, Jeffrey O. 2006. *System Requirements Analysis*. Burlington, MA: Elsevier Inc.
Introduction to Systems Engineering	Sage, Andrew P, and James E Armstrong Jr. 2000. *Introduction to Systems Engineering*. Wiley Series in Systems Engineering. New York: John Wiley & Sons.
Handbook of Systems Engineering and Management	Sage, Andrew P, and William B. Rouse (eds). 2009. *Handbook of Systems Engineering and Management*, 2nd ed. Wiley Series in Systems Engineering. New York: John Wiley & Sons.
Practices as Common Sense	Sobkiw, Walter. 2011. *Systems Practices as Common Sense*. Cherry Hill, NJ: CassBeth
3.5 Cost Cutting Technical Methods	
4 Technical Management Disciplines	
Introduction to Systems Engineering	Sage, Andrew P, and James E Armstrong Jr. 2000. *Introduction to Systems Engineering*. Wiley Series in Systems Engineering. New York: John Wiley & Sons.

Reference or Tool	Brief explanation
INCOSE Systems Engineering Handbook: A Guide for System Lifecycle Processes and Activities	Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering Depicts a similar process as Quality Management Process
Systems Engineering and Analysis	Blanchard, Benjamin S, and Wolter J Fabrycky. 1998. *Systems Engineering and Analysis*. 3rd ed. Upper Saddle River, NJ: Prentice-Hall Inc. Provides more information on the Pareto chart, including constructing one.
4.1 Integrated Technical Management	
Systems Engineering and Analysis	Blanchard, Benjamin S, and Wolter J Fabrycky. 1998. *Systems Engineering and Analysis*. 3rd ed. Upper Saddle River, NJ: Prentice-Hall Inc. Provides more information on preparing a WBS, schedules, and costs.
Introduction to Systems Engineering	Sage, Andrew P, and James E Armstrong Jr. 2000. *Introduction to Systems Engineering*. Wiley Series in Systems Engineering. New York: John Wiley & Sons. For one possible template for a formal SEMP on a large project, see pages 483-484.
IEEE Standard for Application and Management of the Systems Engineering Process	*IEEE Standard for Application and Management of the Systems Engineering Process*. Standard. New York: The Institute of Electrical and Electronics Engineers. Provides information on a standard SEMP.
4.3 Risk, Issue, and Opportunity Management	
FAA RIO Scorecards	
FAA COTS Risk Mitigation Guide	
4.4 Configuration Management	
FAA Order 1800.66 “National Airspace System Configuration Management Policy”	“National Airspace System Configuration Management Policy”
EIA 649 “National Consensus Standard for Configuration Management”	“National Consensus Standard for Configuration Management”
4.7 Verification and Validation Processes	
Verification & Validation Guidelines	FAA AMS Lifecycle Verification and Validation Guidelines
Test & Evaluation Guidelines	FAA Test and Evaluation Process Guidelines
Test & Evaluation Handbook	Test and Evaluation Handbook

7 Acronym List & Glossary

7.1 Acronym List

A

ACAT	Acquisition Category
ADS-B	Automatic Dependent Surveillance – Broadcast
AMS	Acquisition Management System
ANSI	American National Standards Institute
AO	Authorizing Official
APB	Acquisition Program Baseline
ASR	Airport Surveillance Radar
AT	Air Traffic (organization within the FAA)
ATC	Air Traffic Control
ATM	Air Traffic Management
ATO	Air Traffic Organization

B

BCAR	Business Case Analysis Report
BOE	Basis of Estimate
BPMN	Business Process Management Notation

C

C&A	Certification and Accreditation
CA	Certifying Agent
CAA	Clean Air Act
CCB	Configuration Control Board
CCD	Configuration Change Decision
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CFR	Code of Federal Regulations
CHI	Computer-Human Interaction
CI	Configuration Item
CM	Configuration Management
CMP	Configuration Management Plan
CMTD	Concept Maturity and Technology Development
Comm, Comms	Communications

ConOps	Concept of Operations
COTS	Commercial-Off-The-Shelf
CPR	Critical Performance Requirements
CRD	Concept and Requirements Definition
CSA	Comparative Safety Assessment
CSA	Configuration Status Accounting
CSAR	Configuration Status Accounting Report
CTE	Critical Technology Element
CWA	Clean Water Act

D

DA	Decision Analysis
DAA	Designated Approving Authority
DAG	Defense Acquisition Guidebook
DAR	Design Analysis Report
DAU	Defense Acquisition University
DC	Direct Current
Dept	Department
DID	Data Item Description
DM	Data Management
DoD, DOD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DOORS	Dynamic Object-Oriented Requirements System
DOT	Department of Transportation
DR&A	Data Reduction & Analysis
DT	Development Test

E

E^3	Electromagnetic Environmental Effects
EA	Enterprise Architecture
ECP	Engineering Change Proposal
EEE	Electrical, Electronic, and Electrochemical
EM	Electromagnetic
EMC	Electromagnetic Compatibility
EME	Electromagnetic Environment
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EMS	Electromagnetic Susceptibility

Eng	Engineering
ESD	Electrostatic Discharge
Est	Estimate
EVM	Earned Value Management
EXT	External

F

FA	Functional Analysis
FAA	Federal Aviation Administration
FAD	Functional Architecture Document
FAST	Federal Aviation Administration Acquisition System Toolset
FBR	Functional Baseline Review
FCA	Functional Configuration Audit
FCC	Federal Communications Commission
FFBD	Functional Flow Block Diagram
FIA	Final Investment Analysis
FIPS	Federal Information Processing Standard
FISAA	Federal Information Security Amendments Act
FISMA	Federal Information Security Management Act
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode and Effects Criticality Analysis
FMO	Frequency Management Officer
FOIA	Freedom of Information Act
fPR	Final Program Requirements
fPRD	Final Program Requirements Document
FTA	Fault Tree Analysis

G

GA	General Aviation
GAO	General Accountability Office
Govt	Government
GPS	Global Positioning System
GSA	General Services Administration

H

HAW	Hazard Analysis Worksheet
HCI	Human-Computer Interface
HDBK	Handbook

HDR	Hardware Discrepancy Report
HERF	Hazard of EM Radiation to Fuels
HERP	Hazard of EM Radiation to Personnel
HF	Human Factors
HFE	Human Factors Engineering
HFWG	Human Factors Working Group
HHA	Hazard Health Assessment
HMM/EE	Hazardous Material Management / Environmental Engineering
HPI	Human Performance Interface
HSI	Human System Interface
HVAC	Heating, Ventilating, and Air Conditioning
HWCI	Hardware Configuration Item

I

IA	Investment Analysis
IARD	Investment Analysis Readiness Decision
IARR	Investment Analysis Readiness Review
IAT	Investment Analysis Team
IBR	Integrated Baseline Review
ICAO	International Civil Aviation Organization
ICD	Interface Control Document
iCMM	Integrated Capability Maturity Model
ICR	Interface Change Request
ID	Identification
IDA	Investment Decision Authority
IDEF	Integrated Definition for Function Modeling
IEEE	Institute of Electrical and Electronics Engineers, Inc.
I/F	Interface
IFPP	Information for Proposal Preparation
IG	Inspector General
IIA	Initial Investment Analysis
IID	Initial Investment Decision
ILS	Integrated Logistical Support
ILSP	Integrated Logistical Support Plan
ILSPG	Integrated Logistics Support Process Guide
IM	Interface Management
IMS	Integrated Master Schedule
IMT	Integrated Multidisciplinary Team

INCOSE	International Council on Systems Engineering
I/O	Input - Output
IOA	Independent Operational Assessment
IOC	Initial Operational Capability
iPR	Initial Program Requirements
iPRD	Initial Program Requirements Document
iRD	Initial Requirements Document
IRD	Interface Requirements Document
ISAP	Implementation Strategy and Planning
ISD	In-Service Decision
ISE	Information Security Engineering
ISEF	Integrated Systems Engineering Framework
ISO	International Organization for Standardization
ISP	Integrated Safety Plan
ISPD	Integrated Safety Plan Document
ISPR	In-Service Performance Review
ISR	In-Service Review
ISS	Information Systems Security
ISSM	Information System Security Manager
ISSP	Information Systems Security Plan
IT	Information Technology
ITP	Integrated Technical Planning
ITS	Intelligent Transportation System
IWG	Interface Working Group

J

JRC	Joint Resources Council

K

KSA	Knowledge, Skills, and Abilities
KSN	Knowledge Sharing Network

L

LCE	Lifecycle Engineering
LCP	Lifecycle Plan
LOM	Level of Maturity

M

M&C	Monitor & Control
MCI	Master Configuration Index
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MOE	Measure of Effectiveness
MOU	Memorandum of Understanding
MRS	Mature Requirements Statement
MTBF	Mean Time Between Failure
MTTF	Mean Time to (Initial) Failure
MTTR	Mean Time To Restore
MTTRS	Mean Time To Restore Service
MVP	Master Verification Plan

N

N^2	N-squared (used to denote an N by N open field matrix)
N/A	Not Applicable
NAILS	National Airspace Integrated Logistics Support
NAPRS	National Airspace Reporting System
NARP	National Aviation Research Plan
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NATCA	National Association of Air Traffic Controllers
NAS EA	NAS Enterprise Architecture
NCP	NAS Change Proposal
NDI	Non-developmental Item
NESHAP	National Emission Standards for Hazardous Air Pollutants
NEXRAD	Weather surveillance radars
NIST	National Institute of Standards and Technology
NPDES	National Pollutant Discharge Elimination System
NTIA	National Telecommunications and Information Administration

O

OEA	Operational Environmental Assessment
OMB	Office of Management and Budget
ORD	Operational Readiness Date
OSA	Operational Safety Assessment
OSED	Operational Services and Environmental Description

O&SHA	Operating and Support Hazard Analysis
OSHA	Occupational Safety and Health Administration
OT	Operational Test
OT&E	Operational Test & Evaluation
OV	Operational View

P

PA	Process Area
PAT	Production Acceptance Test
PBM	Process-Based Management
PCA	Physical Configuration Audit
PDCA	Plan, Do, Check, Act
PDR	Preliminary Design Review
PDSA	Plan, Do, Study, Act
PHA	Preliminary Hazard Analysis
PID	Probability Impact Diagram
PIR	Post Implementation Review
Pkg	Package
PLA	Program Level Agreement
PMBOK®	Project Management Body of Knowledge
PMI	Project Management Institute
PMO	Program Management Office
PPM	Program Performance Measurement
pPR	Preliminary Program Requirements
pPRD	Preliminary Program Requirements Document
POA&M	Plan of Action & Milestones
PRD	Program Requirements Document
PRR	Product Readiness Review
PRS	Primitive Requirements Statement
PSP	Program Safety Plan
P-Static	Precipitation Static
PT	Product Team
PTR	Program Trouble Report
PUB	Publication

Q

QA	Quality Assurance
QE	Quality Engineering

QFD	Quality Function Deployment
QMS	Quality Management System
Qtr	Quarter

R

RAA	Responsibility, Authority, and Accountability
RADHAZ	Hazards of Electromagnetic Radiation
RAM	Requirements Allocation Matrix
RCRA	Resource Conservation and Recovery Act
RD	Requirements Document
Ref	Reference
RF	Radio Frequency
RFA	Request for Action
RFD	Request for Deviation
RFI	Radio Frequency Interference
RFP	Request for Proposal
RFW	Request for Waiver
RIO	Risk, Issue, and Opportunity
RM	Requirements Management
RMA	Reliability, Maintainability, Availability
RMB	Risk Management Board
RMP	Risk Management Plan
ROM	Rough Order of Magnitude
RPD	Resource Planning Document
RSA	Research and Systems Analysis
RTCA	RTCA, Inc.
RVCD	Requirements Verification Compliance Document

S

SA	System Architect
SAE	Society of Automotive Engineers
SAR	System Analysis Recording
SARP	Standards and Recommended Practices
SAT	Site Acceptance Testing
SBS	Surveillance Broadcast Service
SCAP	Security Certification and Authorization Package
SDR	System Design Review
SE	Systems Engineering or Systems Engineer

SEM	Systems Engineering Manual
SEMP	Systems Engineering Management Plan
SGA	Service-Gap Analysis
SHA	System Hazard Analysis
SIAR	SE Investment Analysis Review
SIR, SIRS	Screening Information Request(s)
SLC	System Lifecycle
SLMN	Service Level Mission Need
SLS	System-Level Specification
SME	Subject Matter Expert
SMS	Safety Management System
SOA	Service-Oriented Architecture
SOC	Service Operations Center
SOP	Standard Operating Procedure
SoS	System of Systems
SOW	Statement of Work
SP	Special Publication
SPICE	Software Process Improvement Capability Determination
SQA	Software Quality Assurance
SQAP	Software Quality Assurance Plan
SRMGSA	Safety Risk Management Guidance for System Acquisition
SRMTS	Safety Risk Management Tracking System
SRR	System Requirements Review
SRVT	Safety Requirements Verification Table
SSAR	System Safety Assessment Report
SSE	System Safety Engineering
SSH	System Safety Handbook
SSHA	Subsystem Hazard Analysis
SSMP	System Safety Management Plan
SSPP	System Safety Program Plan
SSR	System Specification Review
STD	Standard
STLSC	Service Thread Loss Severity Category
SV	System View
SYN	Synthesis

T

TBD	To be determined

T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TI	Technology Insertion
TIM	Technology Interchange Meeting
TOPSIS	Technique for the Order of Prioritization by Similarity to Ideal Solution
TPM	Technical Performance Measurement (or Measure)
TPP	Technical Performance Parameter
TRA	Technology Readiness Assessment
TRR	Test Readiness Review
TS	Trade Studies

U

UML	Unified Modeling Language

V

VRR	Verification Readiness Review
VRTM	Verification Requirements Traceability Matrix
V&V	Validation and Verification

W

WAAS	Wide Area Augmentation System
WBS	Work Breakdown Structure
WJHTC	William J. Hughes Technical Center
WSDD	Web Service Description Document
WSRD	Web Service Requirements Document

7.2 Glossary

Term	Definition
Activity	A set of actions that consume time and resources and whose performance is necessary to achieve or contribute to the realization of one or more outcomes. *(ISO/IEC 15288)*
Allocated Baseline	The approved documentation describing a CI's functional, performance, interoperability, and interface requirements that are allocated from those of a system or higher level configuration item; interface requirements with interfacing configuration items; and the verifications required to confirm the achievement of those specified requirements. *(MIL-STD-973)*
Allocation	Top-down distribution of system-level requirements to the subsystem, element, component, or to the project team that delegated to meet the requirement. Allocation is also the assignment of performance requirements to functions. *(Refer to SEM 4.3)*
Analysis	Logical examination or study of a system to determine the nature, relationships, and interaction of its parts and environment. *(FAA SEM 4.1)*
AND	(Functional Analysis) A condition where all preceding or succeeding paths are required. *(FAA SEM 4.4)*
Availability	The probability that a system or constituent piece will be operational during any randomly selected period of time, or, alternatively, the fraction of the total available operating time that the system or constituent piece is operational. *(FAA SEM 4.8.2)*
Baseline	An agreed-to description of the attributes of a product at a point in time, which serves as a basis for defining change. *(ANSI/EIA-649-1998)*
Behavior Diagram	Graphical representation of system dynamics that incorporates system responses to inputs. A type of functional flow diagram. The behavior diagram differs from functional flow block diagrams in that behavior diagrams contain data flow and control elements. *(See Functional Flow Block Diagram.)*
Change	Any alteration to a product or its released configuration documentation. A configuration change may involve modification of the product, product information and associated interfacing products. *(ANSI/EIA-649-1998)*
Component	A clearly identified (set of) part of the product being designed or produced. *(FAA SEM 2.2)*
Computer Software Component	A functionally or logically distinct part of a CSCI, typically an aggregate of two or more software units. *(FAA SEM 2.2)*
Computer Software Configuration Item	An aggregation of software that is designed for configuration management and treated as a single entity in the Configuration Management process. *(FAA SEM 2.2)*

Term	Definition
Computer Software Unit	An element specified in the design of a CSC that is separately testable or able to be compiled. *(FAA SEM 2.2)*
Concept of Operations (ConOps)	Description of what is expected from the system, including its various modes of operation and time-critical parameters. *(FAA SEM 4.3)*
Configuration Control Board	An Agency-authorized forum for establishing configuration management baselines and for reviewing and acting upon changes to these baselines. A CCB ensures the functional and operational integrity of a baseline through the establishment and enforcement of effective change management and control practices and processes. *(FAA SEM 4.11)*
Configuration Identification	The systematic process of selecting product attributes, organizing associated information about the attributes, and stating those attributes. It includes assigning and applying unique identifiers for the product and its associated documentation, as well as maintaining document revision relationships to the product configurations. *(FAA SEM 4.11)*
Configuration Item	Aggregation of hardware, software, processed materials, services, or any of its discrete parts that is demonstrated for configuration management and treated as a single entity in the configuration management process. *(FAA SEM 4.11)*
Configuration Management	A management process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life. *(ANSI/EIA-649-1998)*
Configuration Status Accounting (CSA)	The systematic recording and reporting of system or product configuration status. Configuration Status Accounting includes baseline change status and history for all items shown in the Master Configuration Index from initial delivery to end of product service. *(FAA SEM 4.11)*
Constraint	Internal or externally imposed boundary conditions which place limits within which the system or process must remain. *(FAA SEM 4.3)* A restriction, limit, or regulation, or, a type of requirement that is not tradable against other requirements. *(EIA Standard 731*)
Control Gate	A formal decision point along the lifecycle that are used by the system owner and stakeholders to determine if the current phase of work has been completed and the team is ready to move into the next phase of the lifecycle. *(FAA SEM 4.2.6)*
Critical Design Review	Formal technical review conducted to evaluate the completeness of the design, its interfaces, and suitability to start initial manufacturing. *(FAA SEM 3.3)*
Decomposition	Partitioning/dividing a requirement into its lower-level discrete elements or parts. (Refer to SEM 4.3)

Term	Definition
Demonstration	Type of verification accomplished by operation, adjustment, or reconfiguration of items performing their design functions under specific scenarios. It is similar to test except that it does not require instrumentation. *(FAA SEM 4.12)*
Demonstrated Performance	The ability of an analysis to produce results that compare favorably with results obtained from the system being modeled over common areas of performance. *(FAA SEM 4.9)*
Derived Requirements	Any requirement that is not explicitly identified by the Customer or Stakeholder. *(Refer to SEM 4.3)*
Design Analysis Report	A report that documents the results of a specific Specialty Engineering analysis with rationale. Each DAR contains a description of the system's special characteristics, a list of existing requirements that have undergone the Validation and Verification process, residual risks, and candidate requirements found as a result of the analysis. *(FAA SEM 4.3)*
Deviation	Specific, written authorization, granted prior to the manufacture of an item, to depart from a particular requirement(s) of an item's current approved configuration documentation for a specific number of units or a specified period of time. (A deviation differs from an engineering change in that an approved engineering change requires corresponding revision of the item's current approved configuration documentation, whereas a deviation does not.) *(MIL-STD-973)*
Digital Data	Information prepared and maintained by electronic means and provided by electronic data access, interchange, transfer, or on electronic media. *(FAA SEM 4.11)*
Digital Device	Any unintentional radiator (device or system) that generates and uses timing pulses at a rate in excess of 9000 pulses (cycles) per second and uses digital techniques . . . *(FCC – Refer to SEM 4.8.4)*
Disposal	*(Lifecycle perspective)* All activities associated with disposal management, dismantlement/demolition/removal, restoration, degaussing, or destruction of storage media and salvage of decommissioned equipment, systems, or sites. *(FAA SEM 4.13)*
Effectivity	Designation defining the point in time, an event, or a product range (e.g., serial, lot number, model, date) at which changes or variances to specific products are to be effected. The authorized and documented point of usage for a specific configuration of a part/assembly/installation, etc. *(Refer to SEM 4.11)*
Electromagnetic Compatibility	The ability of a system to function within its electromagnetic environment and, itself, not be a source of troublesome electromagnetic interference. *(American National Standards Institute (ANSI) C63.14)*

Term	Definition
Electromagnetic Environment	Consists of the systems and other elements (such as humans and nature) that exist within the area that a given system is (or is to be) operated. *(American National Standards Institute (ANSI) C63.14)*
Electromagnetic Environmental Effects (E^3) Engineering	The technical discipline dealing with safe and efficient operation of electronic devices regarding radiated and conducted electromagnetic emissions. This includes both a given system's ability to deal with such emissions from its operational environment and how the device itself affects that environment. *(FAA SEM 4.8.4)*
Electromagnetic Pulse	An intense burst of electromagnetic interference caused by a nuclear explosion. Such a pulse may damage sensitive electronic systems or cause them to temporarily malfunction. *(American National Standards Institute (ANSI) C63.14)*
Electromagnetic Susceptibility	The weaknesses or lack of resiliency a system may have to certain electromagnetic conditions. *(American National Standards Institute (ANSI) C63.14)*
Electrostatic Discharge	An unintentional transfer of static electricity from one object to another. *(American National Standards Institute (ANSI) C63.14)*
(System) Element	An integrated set of components that comprise a defined part of a subsystem (e.g., the fuel injection element of the propulsion subsystem) *(FAA SEM 2.2)*.
Enabling System	A system that complements a system-of-interest during its lifecycle stages but does not necessarily contribute directly to its function. *(ISO/IEC 15288)*
Enterprise	An organization that exists to perform a specific mission and to achieve associated goals and objectives. *(NAS EA Course)*
(NAS) Enterprise Architecture	A strategic and evolutionary plan for modernizing the NAS that supports investment analysis tradeoffs. It focuses on defining and delivering the services that meet aviation industry and public needs, which it accomplishes by decomposing the services into capabilities that are the functions and activities necessary to deliver a service. Each capability is defined by the operational improvements required to deliver the capabilities. Each operational improvement is defined in terms of the mechanisms required to provide each step. Finally, each mechanism is defined in terms of the people, systems, and support activities provided by the procuring office. *(FAA SEM 4.3)*
Environment	Natural and induced conditions experienced by a system, including its people, product, and processes. *(Refer to SEM 4.4)*
Exclusive OR	(Functional Analysis) A condition where one of multiple preceding or succeeding paths is required, but not all. *(FAA SEM 4.4)*

Term	Definition
Extensibility	The ability of a design alternative to serve new or multiple uses. (As opposed to flexibility) *(FAA SEM 4.5)*
Facility Baseline	The information needed to identify and control changes as well as record configuration and change implementation status of all CIs under Regional CCB authority. *(FAA SEM 4.11)*
Failure Modes and Effects Analysis	An evaluation process for analyzing and assessing the potential failures in a system, i.e. a systematic method of identifying the failure modes of a system, a constituent piece, or function and determining the effects on the next higher level of the design. *(FAA SEM 4.8.2)*
Failure Modes and Effects Criticality Analysis	An analysis method used to identify potential design weaknesses through a systematic analysis approach that considers all possible ways in which a component may fail (the modes of failure); possible causes for each failure; likely frequency of occurrence; criticality of failure; effects of each failure on systems operation (and on various system components); and any corrective action that may be initiated to prevent (or reduce the probability of) the potential problem from occurring in the future. *(FAA SEM 4.8.2)*
Federal Aviation Administration Order	A permanent directive on individual subjects or programs that apply to the FAA. It directs action or conduct using action verbs. Orders also prescribe policy, delegate authority, and empower and/or assign responsibility for compliance with stated requirements or direction. Orders empower or direct only FAA personnel and carry no weight with contractors. *(FAA SEM 4.3)*
Flexibility	The ability (of a design alternative) to adapt to and accommodate growth needs (as opposed to extensibility) *(FAA SEM 4.5)*
Function	Characteristic action, or activity that needs to be performed to achieve a desired system objective (or stakeholder need). *(FAA SEM 4.4)*
Function name	An action that describes the desired system behavior. A *function name* is stated in the form of an action verb followed by a noun or noun phrase. *(FAA SEM 4.4)*
Functional Analysis	A System Engineering process that translates stakeholders' needs into a sequenced and traceable functional architecture. *(FAA SEM 4.1)*
Functional Architecture	Hierarchical arrangement of functions and interfaces providing a complete representation of the system from a performance and behavioral perspective. *(FAA SEM 4.4)*
Functional Baseline	The approved documentation describing a system's or item's functional, interoperability, and interface characteristic, and the verifications required to demonstrate the achievement of those specified requirements. *(MIL-STD-973)*.

Term	Definition
Functional Baseline Review	A formal review to ensure that requirements have been completely and properly identified and that there is a mutual understanding between the implementing organization and stakeholders. *(FAA SEM 3.3)*
Functional Configuration Audit	A formal review to verify that the system and all subsystems can perform all of their required design functions in accordance with their functional and allocated configuration baselines. *(FAA SEM 3.3)*
Functional Decomposition	Approach to reducing functional complexity by allocating functionality and interfaces to more readily understood and managed sublevel functions. *(FAA SEM 4.4)*
Functional Flow Block Diagram	A Multi-tier, time-sequenced, step-by-step diagram that defines the detailed, step-by-step operational and support sequences for systems. (See also Behavior Diagram.) *(FAA SEM 4.4)*
Functional Interface	Logical or physical association between functions that allows transmission of a quantity across a boundary. Quantities may include electrical, hydraulic, and pneumatic power; mechanical forces and torques; gases; heat; vibration, shock, and loads; data; and other quantities. *(FAA)*
Handbook	A guidance document that contains information or guidelines for use in design, engineering, production, acquisition, and/or supply management operations. These documents present information, procedural and technical use data, or design information related to processes, practices, services, or commodities. *(FAA SEM 4.3)*
Hazard	Any real or potential condition that can cause injury, illness, or death to people; damage to, or loss of, a system (hardware or software), equipment, or property; and/or damage to the environment. *(FAA SEM 4.8.1)*
Hazardous Material Management/ Environmental Engineering	The mechanism applied within the system engineering process to ensure a program's ongoing compliance with applicable environmental laws. It is also the process designed to provide early, pre-deployment planning and coordination to minimize the negative impacts that site-specific environmental conditions may have on a program's operability. *(FAA SEM 4.8.7)*
Human Factors Engineering	A multidisciplinary effort to generate and compile information about human capabilities and limitations, and apply that information to (the design and acquisition of complex systems) produce safe, comfortable, and effective human performance. *(FAA SEM 4.1)*
In-Service Performance Review	A formal technical review to characterize in-Service technical and operational health of the deployed system by providing an assessment of risk, readiness, technical status, and trends in a measurable form that will substantiate in-Service support, budget priorities, and/or possible disposal. *(FAA SEM 3.3)*

Term	Definition
Inclusive OR	(Functional Analysis) A condition where one, some, or all of the multiple preceding or succeeding paths is required. *(FAA SEM 4.4)*
Inspection	Type of verification method accomplished by visually examining the item, reviewing descriptive documentation, and comparing the appropriate characteristics with predetermined standards to determine conformance to requirements without the use of laboratory equipment or procedures. *(FAA SEM 4.12)*
Integrity of Analyses	A disciplined process applied throughout a program to ensure that analyses provide the required levels of fidelity, accuracy, and confirmed results in a timely manner. Integrity is ensured by competent users iteratively applying a validated set of tools to a clearly defined data set. *(FAA SEM 4.1 and 4.9)*
Integrated Logistics Support (ILS)	a structured discipline for defining support constraints and acquiring support assets so that fielded products can be operated, supported, and maintained effectively over their entire service life. (FAA SEM 4.13)
Integrated Technical Planning	The tactical and strategic means of defining problems, forecasting conditions, and coordinating program elements to maximize program focus on providing superior products and services. *(Forsberg, Mooz, and Cotterman)*
Integration	The progressive linking and testing of system components to merge their functional and technical characteristics into a comprehensive, interoperable system. *(Institute for Telecommunications, US Dept of Commerce)*
Interface	The performance, functional, and physical attributes required to exist at a common boundary. *(FAA SEM 4.1)*
Interface Control Document (ICD)	A design document that describes the detailed, as-built implementation of the functional requirements contained in the IRD *(FAA SEM 4.7)*
Interface Management	An element of System Engineering (SE) that helps to ensure that all the pieces of the system work together to achieve the system's goals and continue to operate together as changes are made during the system's lifecycle. *(FAA SEM 4.1)*
Interface Requirements	Requirements specifying the performance, functional or physical attributes that are required to exist at a common boundary. This boundary can exist between two or more functions, systems, system elements, configuration items, or systems. *(FAA SEM 4.7)*
Interface Requirements Document (IRD)	Document that provides FAA interface requirements between two elements, including type of interface (electrical, pneumatic, hydraulic, etc.) and the interface characteristics (functional or physical). *(FAA SEM 4.7)*

Term	Definition
Interface Working Group (IWG)	A forum for discussing interface issues. IWG meetings serve two purposes: to ensure effective, detailed definition of interfaces by all cognizant parties, and to expedite baselining of initial IRDs, ICDs, and subsequent drawing changes by encouraging resolution of interface issues. *(FAA SEM 4.7)*
Investment Program	A sponsored, fully funded effort initiated at Final Investment Decision of the lifecycle management process by the investment decision authority in response to a priority agency need. The goal of an investment program is to field a new capability that satisfies performance, cost, and schedule targets in the acquisition program baseline and benefit targets in the business case analysis report. *(FAA FAST)*
Lifecycle	Entire spectrum of activity for a given system, commencing with the identification of a need and extending through system design and development, production and/or construction, operational use, sustaining support, and system retirement and phase-out. *(FAA SEM 4.1)*
Lifecycle Engineering	An objective process to evaluate the constraints and dependencies associated with developing and operating a product or service, while seeking to maximize the product or service's value while minimizing the cost of ownership of the product or service over the entire lifecycle. *(FAA SEM 4.1)*
Maintainability	The measure of the ability of a failed system or constituent piece to be restored to its fully operational status. *(FAA SEM 4.8.2)*
Master Configuration Index	A list of all baselined systems, equipment and software currently operational or under procurement for the National Airspace System (NAS) with current approved baseline documentation. *(FAA SEM 4.3)*
Mature Requirement Statement	A written statement of a requirement in one or more complete sentences in a familiar language (normally English) using the idiom of a particular business sector, such as air traffic control or avionics. *(FAA SEM 4.3)*
Mean Time Between Failure (MTBF)	The mean number of life units during which all parts of the system or constituent piece perform within their specified limits, during a particular measurement interval under stated conditions. *(FAA SEM 4.8.2)*
Mean Time To Failure (MTTF)	The average time for a system to fail initially, based on the behavior of similar systems, operated under specified conditions for the duration of a specified time interval. *(FAA SEM 4.8.2)*
Mean-Time-To-Restore	The average total elapsed time from initial failure to resumption of operation. *(FAA SEM 4.8.2)*
Measure of Effectiveness (MOE)	Measures of operational effectiveness and suitability in terms of operational outcomes that identify the most critical performance requirements to meet system-level mission objectives. *(FAA SEM 4.3)*

Term	Definition
Mechanism	A control gate that assesses the progress of the system against criteria established for a given point in the system's lifecycle. *(FAA SEM 4.2.6)*
Minimum Aviation System Performance Standard (MASPS)	A standard (published by RTCA) that address the user-level service requirements used to qualify an aviation system for operational acceptance and to allocate requirements for the subsystems (including avionics). The standards provide information that explains the rationale for system characteristics, operational goals, requirements, and typical applications. *(FAA SEM 4.3)*
Minimum Operational Performance Standard (MOPS)	A standard (published by RTCA) that describes typical (avionics) equipment applications and operational goals and establishes the basis for required performance and test procedures for verification under a common set of standards. Definitions and assumptions essential to proper understanding are provided, as well as installed equipment tests and operational performance characteristics for equipment installations. The MOPS also provide information that explains the rationale for equipment characteristics and stated requirements. *(FAA SEM 4.3)*
(Service level) Mission Need	A document that translates a ConOps into the needs and requirements of the users and service providers. It identifies the decision factors relevant to a capability shortfall or a technological opportunity to satisfy a mission more efficiently or effectively. *(Refer to SEM 4.4)*
Model	Representation of an actual or conceptual system that involves mathematics, logical expressions, or computer simulations that may be used to predict how the system might perform or survive under various conditions or in a range of hostile environments. *(See also Simulation)*
Module (Computer Software)	A program unit that is discrete and identifiable with respect to compiling, combining with other units, and loading. *(FAA SEM 2.2)*
N^2 Diagram	Visual matrix representing functional or physical interfaces between system elements. *(FAA SEM 4.4)*
National Air Space (NAS)	the overall environment in which aircraft operate, including aircraft, pilots, tower controllers, terminal area controllers, en route controllers, oceanic controllers, maintenance personnel, and airline dispatchers, as well as the associated infrastructure (facilities, computers, communications equipment, satellites, navigation aids, and radars) *(FAA SEM 2.2)*
Operational Baseline	The Product Baseline adapted to local conditions, i.e. the approved technical documentation representing installed operational hardware and software. *(FAA SEM 4.11)*
Operational Services and Environmental Description (OSED)	A comprehensive, holistic system description that describes the services, environment, functions, and mechanizations that form a system's characteristics. *(FAA SEM 4.4)*
Order (FAA)	A permanent directive on individual subjects or programs that apply to the FAA. It directs action or conduct using action verbs. *(FAA SEM 4.3)*

Term	Definition
Precipitation-Static (P-Static)	The buildup of static electricity resulting from an object's exposure to moving air, fluid, or tiny solid particles (e.g., snow or ice). *(American National Standards Institute (ANSI) C63.14)*
Part	One, two, or more pieces joined together to make a component; these pieces are not normally subject to disassembly without destruction or impairment of designed use – the lowest level of separately identifiable items within a system. *(FAA SEM 2.2)*
Performance	Quantitative measure characterizing a physical or functional attribute relating to the execution of an operation or function. Performance attributes include quantity (how many or how much), quality (how well), coverage (how much area, how far), timeliness (how responsive, how frequent), and readiness (availability, mission/operational readiness). Performance is an attribute for all systems, people, products, and processes, including those for development, production, verification, deployment, operations, support, training, and disposal. Thus, supportability parameters, manufacturing process variability, reliability, and so forth are all performance measures.
Physical Architecture	Hierarchical arrangement of hardware and/or software components along with associated interfaces depicting the physical definition of the system. *(FAA SEM 4.4)*
Physical Configuration Audit	the formal examination of the "as-built" configuration of a configuration item against its technical documentation to establish or verify the configuration item's product baseline. *(MIL-STD-973)*
Practice (ICAO recommended)	Identical to a standard except that it is not considered necessary - only desirable. *(See Standard (ICAO)below)*
Preliminary Design Review	Formal technical review of initial design concepts and documentation to confirm the preliminary design logically follows the SRR findings, meets the requirements, and to further define physical and functional interface requirements. *(FAA SEM 3.3)*
Primitive Requirement Statement	A form of a requirement statement that has no punctuation or formal sentence structure and is not written in a formal specification style. *(FAA SEM 4.3)*
Process	Set of interrelated or interacting activities that transform inputs into outputs. *(ISO/IEC 15288)*
Product	Whole system, entity, or process being designed, developed, and/or produced. *(FAA SEM 4.3)*
Program	A group of related projects managed in a coordinated way to obtain benefits and control not available from managing them individually. *(PMI's PMBoK)*

Term	Definition
Project	A temporary endeavor undertaken to create a unique product, service, or result. In the FAA the term is used for work that is not part of a Capital Investment Plan (CIP) program. *(PMI's PMBoK)*
Product Baseline	The configuration of the system or product being delivered to the customer. It is comprised of the combined performance/design documentation utilized for the production/procurement of the CI. This documentation package incorporates the allocated baseline documents describing a CI's functional, performance, interoperability and interface requirements and the verifications required to confirm the achievement of those specified requirements. It also includes additional design documentation, ranging from form and fit information about the proven design to a complete design disclosure package, as is deemed necessary for acquisition of the CI. *(MIL-STD-973)*
Product Definition	The aggregation of configuration item (CI) descriptions and supporting documentation necessary to define a product. This includes all hardware configuration items (HWCI) and computer software configuration items (CSCI). After the product baseline is established, the product definition includes ALL documentation required to design, build, assemble, test, modify, repair or support the product. This includes tooling, planning, analyses, parts lists, material standards and other product related items. *(FAA SEM 4.11)*
Quality Engineering	An objective analysis of all planned and systematic activities to ensure that a product or service fulfills requirements and is of the highest quality. *(FAA SEM 4.8.5)*
Quality Function Deployment	Method for capturing and delineating requirements based on identifying what is desired by the customer or stakeholder, along with how that desire may be satisfied. *(Refer to SEM 4.6)*
Reference Analyses	A set of authorized, validated analyses (certified in the case of simulations) established as reference analysis methods for use in subsequent analyses. *(FAA SEM 4.9)*
Reference Model	The function modeled in one particular validated tool is identified as a standard for comparison. A reference model is established to capitalize on primary expertise in specific areas of performance and to provide consistency at the subsystem level. *(FAA SEM 4.9)*
Reference Database	A database that represents the selected subsystem performance through tabulated values. *(FAA SEM 4.9)*
Reference Check Case	A representative set of conditions or characteristics for a situation under study that is used as the basis for certification comparison. *(FAA SEM 4.9)*

Term	Definition
Reliability	Ability of a system and its parts to perform its mission without failure, degradation, or demand on the support system. It is generally characterized by the Mean-Time-Between-Failure (MTBF). *(FAA SEM 4.8.2)*
Requirement	An essential characteristic, condition or capability that shall be met or exceeded by a system or a component to satisfy a contract, standard, specification, or other formally imposed document. *(FAA SEM 4.3)*
Requirement Set	An aggregate of requirements for a system that specifies its characteristics in totality. *(FAA SEM 4.3)*
Requirements Analysis	The determination of system specific characteristics based on analyses of customer needs, requirements, and objectives; missions; projected utilization environments for people products and processes; constraints; and measures of effectiveness. *(FAA SEM 4.3)*
Requirements Document	Collection of requirements and related information/attributes presented in a user-defined format. *(FAA SEM 4.3)*
Requirements Management	a process performed throughout a system's lifecycle, to elicit, identify, develop, manage, and control requirements and associated documentation in a consistent, traceable, correlatable, verifiable manner. *(FAA SEM 4.1)*
Requirements Verification Compliance Document	A document that provides evidence of system design compliance for each product requirement at all levels. *(FAA SEM 4.3)*
Risk	A future event or situation with a realistic (non-zero nor 100 percent) likelihood/probability of occurring and an unfavorable consequence/impact to the successful accomplishment of well-defined goals if it occurs *(FAA SEM 4.1)*
Risk *(Information Security)*	The combination of a threat, its likelihood of successfully attacking a system, and the resulting effects and harm from that successful attack. *(FAA SEM 4.8.6)*
Risk Identification	A systematic effort to uncover possible events or conditions that, if they occur, may hinder achievement of program or organization objectives. *(FAA SEM 4.10)*
Risk Management	An organized, systematic decision-support process that identifies risks, assesses or analyzes risks, and effectively mitigates or eliminates risks to achieve program or organizational objectives. *(FAA SEM 4.1)*
Risk Realization (Date)	The point in time of an event that either makes the risk a real part of the program or eliminates the need to track the risk. *(FAA SEM 4.10)*

Term	Definition
Safety Risk	The composite of predicted severity and likelihood of the potential effect of a hazard. 1. Initial – The predicted severity and likelihood of a hazard's effects or outcomes when it is first identified and assessed; includes the effects of preexisting risk controls in the current environment. 2. Current – The predicted severity and likelihood at the current time. 3. Residual – The remaining predicted severity and likelihood that exists after all selected risk control techniques have been implemented. (FAA Order 8040.4A Safety Risk Management Policy)
SE Investment Analysis Review	A formal SE review to determine if the mission need capabilities shortfall and attendant solution set of alternatives are complete enough to support a Mission Need Decision. *(FAA SEM 3.3)*
Service Organization	A service organization is any organization that manages investment resources regardless of appropriation to deliver services. It may be a service unit, program office, or directorate, and may be engaged in air traffic services, safety, security, regulation, certification, operations, commercial space transportation, airport development, or administrative functions. *(FAA FAST)*
Similarity	Type of verification by analysis. Applicable to components and subsystems similar in characteristics and usage to those on previous systems, and the prior system was qualified to equivalent or greater specifications. *(FAA SEM 4.12)*
Simulation	Execution of a system model to examine the response of the system to injected inputs, usually performed before development of system hardware and software. *(See also Model above) (Refer to SEM 4.12)*
Software	A combination of associated computer instructions and computer data definitions required to enable the computer hardware to perform computational or control functions. *(FAA SEM 2.2)*
Specialty Engineering	A System Engineering domain that defines and evaluates a system's specific areas, features, or characteristics. Specialty Engineering supplements the design process by defining these characteristics and assessing their impact on the program. *(FAA SEM 4.1)*
Specification	A document prepared specifically to support an acquisition that clearly and accurately describes the essential technical requirements for purchased material or products and the criteria for determining whether the requirements are satisfied. *(FAA SEM 4.3)*

Term	Definition
Standard	A document that establishes engineering and technical requirements for processes, procedures, practices, and methods that have been adopted as standard. *(FAA SEM 4.3)* Any specification for physical characteristics, configuration, material performance, personnel, or procedure that is applied uniformly for the safety or regularity of international air navigation and to which the international aviation community conforms. *(ICAO – see FAA SEM 4.3)*
Subsystem	A system in and of itself (reference the system definition) contained within a higher-level system. The functionality of a subsystem contributes to the overall functionality of the higher-level system. The scope of a subsystem's functionality is less than the scope of functionality contained in the higher-level system. *(FAA SEM 2.2)*
Synthesis	The creative process which translates requirements (performance, function, and interface) into alternative solutions resulting in a physical architecture for the "best-value" design solution, made up of people, products, and process solutions for the logical, functional grouping of the requirements. *(FAA SEM 4.1)*
System	An integrated set of constituent pieces that are combined in an operational or support environment to accomplish a defined objective. These pieces include people, hardware, software, firmware, information, procedures, facilities, services, and other support facets. *(FAA SEM 2.2)*
System Boundary	The interface between system elements under design control and elements that are not. *(FAA SEM 4.3)*
System Engineer	Individual who concentrates on the design and application of the whole (system), as distinct from the parts, and who looks at a problem in its entirety, taking into account all the facets and all the variables and relating the social to the technical aspects. *(Ref SEM 1.0)*
Systems Engineering	A discipline that concentrates on the design and application of the whole (system) as distinct from the parts. It involves looking at a problem in its entirety, taking into account all the facets and all the variables and relating the social to the technical aspects. *(FAA SEM 1.0)*
System Engineering Management Plan (SEMP)	A document that identifies what items are to be developed, delivered, integrated, installed, verified and supported. It identifies when these tasks will be done, who will do them, and how the products will be accepted and managed. It also defines the technical processes to be used to produce each of the project's products. *(California Department of Transportation, Systems Engineering Handbook for ITS, V1.1)*
System-of-Interest	The system whose lifecycle is under consideration. *(ISO/IEC 15288)*

Term	Definition
System Requirements Review	A formal review to verify that requirements have been completely and properly identified and are correct. This review can be conducted at different levels, depending on the requirements set being reviewed. *(FAA SEM 4.2.6)*
Technical Performance Measurement	a process to continuously assess and evaluate the adequacy of architecture and design as they evolve to satisfy the requirements and objectives of the program. *(FAA SEM 4.2.6)*
Technical Performance Parameter	A critical technical performance requirement that supports critical operational needs and essentially measures the extent of success or failure of a design to meet those needs. *(FAA SEM 4.2.6)*
Technology Maturity	A measure of the degree to which proposed critical technologies meet program objectives; and, is a principal element of program risk. A technology readiness assessment examines program concepts, technology requirements, and demonstrated technology capabilities in order to determine technological maturity. *(DOD 5000.2)*
Technology Readiness Assessment	A multi-disciplined technical review that assesses the maturity of Critical Technology Elements (CTEs) being considered to address user needs; analyzes operational capabilities & environmental constraints within the Enterprise Architecture (EA) framework. *(FAA SEM 3.3)*
Test	Type of verification accomplished through systematic exercising of the application item under appropriate conditions, with instrumentation, and the collection, analysis, and evaluation of quantitative data. It includes both laboratory and flight tests. *(FAA SEM 4.12)*
Thread	A system input, system output, description of the transformations to be performed, and the conditions under which these transformations are to occur. *(Refer to SEM 4.4)*
Threshold requirement	Those requirements considered so important to satisfying the user needs that a system not meeting them is deemed unnecessary or unacceptable. *(FAA SEM 4.5)*
Traceability	Characteristic by which requirements at one level of design may be related to requirements at another level. Traceability encompasses the relationship between a performance requirement and the function from which the performance requirement was derived. *(Refer to SEM 4.3)*
Trade Study	Analysis conducted to methodically evaluate a series of design alternatives and recommend the preferred feasible solution(s) that enhance the value and performance of the overall system and/or functions. Each assessment is taken to an appropriate level of detail that allows differentiation between alternatives. *(FAA SEM 4.1)*
Validated (method, model, or tool)	One that has been proven to provide credible results at the associated level of fidelity for a given analysis or study. *(FAA SEM 4.9)*

Term	Definition
Validation	Validation demonstrates whether a product will fulfill its specified purpose when placed in any aspect of its intended environment such as operation, training, manufacturing, maintenance, or support services. The methods employed to accomplish validation can be applied to work products as well as to the product. Work products are selected on the basis of being the best predictors of how well the product and product component will satisfy user needs and the level of risk they present to the program. Validation is performed early and incrementally throughout the product lifecycle, often requiring rigorous analysis to ensure the right product is being procured.determination that the requirements for a product are sufficiently correct and complete. (SAE ARP 4761, 1996FAA AMS Lifecycle Verification and Validation Guidelines 2.0)
Validation Table	A listing of all requirements that describes if a requirement has been validated, where the requirement may be found, source of validation, corrective action to be taken if necessary, and the corrective action owner.
Variance	Specific, written authorization to depart from a particular requirement(s) of a product's current approved configuration documentation for a specific number of units or a specified period of time. (A variance differs from an engineering change in that an approved engineering change requires corresponding revision of the product's current approved configuration documentation, whereas a variance does not.) *(Refer to SEM 4.11)*
Verification	Verification ensures that selected work products, product components, and products meet specified requirements and standards. Verification is inherently an incremental process since it occurs throughout the development of work products and products, beginning with initial concepts, progressing through subsequent changes, and continuing throughout the lifecycle. *(FAA AMS Lifecycle Verification and Validation Guidelines 2.0)*
Verification Readiness Review	A formal review to ensure that all system engineering considerations are satisfied and that the readiness of all support, test, and operational systems is in order to perform the Verification process. *(FAA SEM 3.3)*
Verification Requirements Traceability Matrix	Matrix correlating requirements and the associated verification method(s). The VRTM defines how each requirement (functional, performance, and design) is to be verified, the stage in which verification is to occur, and the applicable verification levels. *(FAA SEM 4.3)*
Waiver	A written authorization to accept an item, which during manufacture, or after having been submitted for inspection or acceptance, is found to depart from specified requirements, but nevertheless is considered suitable for use "as is" or after repair by an approved method.
Work Breakdown Structure	A key element of planning that details the activities to be performed. It is a deliverable oriented grouping of project elements, which organizes and defines the total scope of the project. Each descending level represents an increasingly detailed definition of a project component. *(FAA SEM 4.2)*

8 Appendices

8.1 Appendix A: Special Considerations for System of Systems

The Introduction to the SEM contained a brief introduction to consideration for System of Systems (SoS). Some systems engineers might need or desire more information on SoS. With that in mind, this appendix provides a definition of SoS, a means to identify a SoS apart from other types of systems, and presents a list of known challenges. In addition, the SEM includes some suggestions for SoS engineering and integration of a SoS, based on existing research.

At a minimum, a SoS is fundamentally a system that exists as an amalgamation of other autonomous systems. FAA recognizes a SoS as a distinct entity with a unique set of characteristics and traits. Given this view, there is good reason to call out the NAS as a SoS since it requires special considerations. The SEM accepts a SoS as a unique type of system with a defined user need, resources designated to address the need, and an agency responsibility to address this need.

8.1.1 Identifying a System of Systems

A SoS is a collection of independent systems that work together to achieve some common purpose (DeLaurantis 2005, Manthorpe 1996, Shenhar 2009). The NAS is a very complex SoS since it includes many facilities (e.g. TRACONs, ARTCCs, and airports), systems (e.g. ERAM, TFMS, and SWIM), equipment, and procedures that collectively work together to provide a common service: a safe and efficient flying environment for both commercial and general aviation customers. As such, the NAS, and many of its constituent systems, presents a number of SoS distinguishing characteristics, such as physically distributed systems, functionality that emerges from the connections between systems, system heterogeneity (Kotov 1997), slow evolution over time, and development that is more complex than developing stand-alone systems (Crossley 2004). The union of unique, individual systems, many of which are SoS, within the NAS forms a new SoS with a different function than any one of the individual systems (Shenhar 1997), and the various systems within the NAS can achieve results together that they could not do alone (DeLaurentis 2004, Carlock 2001).

An often cited depiction of SoSs describes a collection of component systems with two additional properties. Each component system must have its own purpose independent of the other systems, and the component systems must maintain their independence (Carlock 1999). Expanding on that description, Boardman and Sauser (Kang 2005) review 41 papers on SoSs to extract commonalities from the definitions. They divide the various traits into common descriptive characteristics, which define a SoS as well as differentiate it from other systems. These five “essential characteristics” are:

- Autonomy - the ability to complete one’s own goals
- Diversity- indicates the goals of each system within the SoS differ
- Belonging- the contribution to the goal of the SoS in exchange for advancing the system’s goals
- Connectivity- implies dynamic connectivity where the systems are interconnected in a robust manner (Baldwin 2011-A, Baldwin 2009)
- Emergence - indicates the presence of some behavior or feature that arises within the SoS but cannot be traced to any one constituent system (Baldwin 2011-A, Kang 2005, INCOSE 2010)

In summary, a SoS, such as the NAS, is a type of system comprising a diverse set of constituent systems with unique contributions. A SoS differs from a traditional system in that a SoS consists of multiple, diverse, autonomous systems, while the constituents of a traditional system are not

autonomous (Baldwin 2011-A). Table 34 illustrates a number of ways that a SoS differs from a traditional system.

Table 34: Differences between SoS and Traditional Systems

Traditional System	System of Systems
Overall system is autonomous but its parts are not	Overall SoS is autonomous as well as its constituent systems
Goals are unique to the system	Goals are unique from the goals of its constituent systems
Behavior specific to system	Resultant complexity of the interconnected systems produces emergent features, in other words behavior that cannot be traced to any constituent system
Parts of a system collaborate only to the extent they are designed	Constituent systems collaborate as needed to help each other reach their goals
Parts of a system are statically connected	Constituent systems may be dynamically connected, joining and separating from the SoS as needed
Each system is unique	SoS is composed of a diversity of constituent systems
A system is more than the sum of its parts but may not necessarily be complex	A SoS exhibits emergent functionality that cannot be traced to any particular constituent system and may be the result of the dynamic connectivity of the constituent system.
Service unit systems such as ERAM, ADS-B, WMSCR, etc.	Current and future NAS (*i.e.*, NextGen)

8.1.2 Types of Systems of Systems

Just as there are many types of systems, there are potentially multiple types of SoS. These five types of SoS may not be exhaustive, but they do give an idea as to how SoSs may differ.

- A **virtual** SoS is a collection of component systems, which are not engineered or acquired to be part of a SoS, but develop the SoS characteristics when connected (Gorod 2008).
- A **collaborative** SoS consists of component systems that willingly interact to fulfill the collective goal (Baldwin 2011-B). In a virtual a collaborative SoS, the integration is relatively straightforward as the systems practically integrate themselves.
- A **chaotic** SoS has no agreed-upon goal and the constituent systems interact as they see fit. The random interactions cause unpredictable behavior (Gorod 2008).
- An **acknowledged** SoS has recognized overall goals but the constituent systems maintain their independence (Baldwin 2011-B). An example of this type of SoS is a federated system, where there is a central program office but the constituent systems participate via documented agreements.
- A **dedicated** SoS is built and integrated for a specific purpose (Baldwin 2011-B). They are consciously designed and engineered from the beginning to be a SoS (Gorod 2008).

8.1.3 Challenges of a System of Systems

A SoS, such as the NAS, poses a number of unique system engineering challenges. These system engineering challenges include the following:

- Autonomy of systems causes each system to operate independently, for the most part (DeLaurentis 2004)

- Requirements regarding the overall SoS functionality are likely to be ambiguous (DeLaurentis 2004)
- Interaction of systems grows exponentially as constituent systems are added to the SoS (DeLaurentis 2004)
- Interfaces conflict and the documentation becomes poorly defined as the interaction of systems grows, and so does the importance of interface management.
- Management of each constituent system overshadows engineering efforts for the SoS (DeLaurentis 2004)
- Fuzzy boundaries within the SoS cause confusion (DeLaurentis 2004)
- Diversity of SoS configurations cause management problems (DeLaurentis 2004)
- SoSs evolve over time and therefore engineering is never finished (Carlock 1999)
- Interoperability of constituent systems causes changes in one system to have unexpected impact on other systems (ODUSD 2008)
- Functionality emerges from the connections between constituent systems (Kotov 1997)
- Test and validation is distributed and federated, which complicates testing (ODUSD 2008)

This list of challenges may not be inclusive as the emergent nature of a SoS can cause any number of challenges. Many of these challenges are already present when dealing with the NAS and its constituent systems and more should be expected with NextGen. For example, one obvious challenge when dealing with any constituent system in a SoS is risk management. Due to the interconnected nature of the systems, a change to one system may ripple through other systems. However, risk management traditionally focuses on the system of interest and generally lacks authority to mitigate risks outside of its domain.

Another example of SoS unique challenges is that System of Systems Engineering (SoSE) typically involves multiple system lifecycles that are not necessarily part of a single acquisition program. Rather, the SoS, such as the NAS and its component systems, may comprise legacy systems, developmental systems in acquisition programs, technology insertion, life extension programs, and systems related to other initiatives. The acquisition of SoS capability generally will not be driven solely by a single organization but rather may involve multiple program offices and support communities (ODUSD 2008). Consequently, lifecycle engineering has a different challenge of managing an architecture that is constantly changing as the SoS evolves. The lifecycle engineers assigned to each constituent system must communicate often in order to be prepared for changes imposed by other systems. Since the SoS evolves with new systems coming on line as old ones are decommissioned, the lifecycle engineering aspect of SoSE must pay greater attention to the disposal process.

Challenges such as these must be addressed as NextGen develops by way of increased collaboration between all parties, including NextGen, NAS and non-NAS programs, and external stakeholders. In any case, this list gives the systems engineer an idea of the difficulties that one may face when engineering aspects of NextGen. SoS discussions may be found in a number of sections within this document that address SoS-related challenges.

8.1.4 System of Systems Engineering (SoSE)

Most, if not all, aspects of classical systems engineering apply in some part to SoS, but classical systems engineering is insufficient to handle all aspects of these complex systems. Since SoSs are different than traditional systems, appropriate engineering techniques need to address them. One of the main differences is the need to focus on the relationships among the constituent systems in addition to the functions of each system. From General Systems Theory, “You cannot sum up the behavior of the whole from the isolated parts, and you have to take into account the relation between the various subordinated systems and systems which are super-ordinated to them in order to understand the behavior of the parts” (Biggiero 2001). This action of considering the whole and the interaction of parts constitutes the systems approach.

In a SoS, the interrelationships caused by the dynamic connections between constituent systems produce many emergent features (Calvano 2004). A systems approach starts to address these interconnections by considering the gaps between systems in addition to the systems themselves. The systems approach can be defined as, “an approach to a problem which takes a broad view, which tries to take all aspects into account, which concentrates on interaction between the different parts of the problem” (Gideon 2005). Yet, the systems approach does not abandon reductionism while emphasizing a more holistic view. Reductionism is a scientific approach that focuses on reducing things to the interactions of the parts, or to more fundamental things. On the other hand, holism considers a system or thing as a whole and may best be summarized as the belief that the whole is more than the sum of the parts. A true systems approach attempts to understand the nature of complex systems by reducing them to the interactions of their parts, i.e., reductionism, while considering the system as a whole, i.e., holism.

Another emergent feature requiring a system approach is the adaptive nature of a SoS. Constituent systems may not integrate in the traditional manner but rather collaborate as needed. Such constituent systems must be designed and managed to optimize the chance for collaboration. Combinations of systems operating together within the SoS contribute to the overall capabilities and the performance and behavior of the SoS can have stronger dependencies than expected between the constituent systems. The individual systems may not have been designed for this level of dependency in their usual course of operation, and SoS capabilities may depend more strongly on emergent behaviors than is usually expected from a single system. As with emergent behaviors of single systems, these behaviors may either improve performance or degrade it.

8.1.5 Integration in System of Systems

It is more difficult to test and assemble a SoS than a single system due to the diverse, autonomous constituent systems. While the constituent systems may meet all assurance requirements, the networking of these systems into a SoS may introduce new vulnerabilities. In addition, the communication system should be explicitly evaluated for security, safety, reliability, and assurance. A SoSE challenge is to leverage the functional and performance capabilities of the constituent systems so as to achieve the desired SoS capability.

The performance of a SoS is dependent not only on the performance of the individual constituent systems but also on their evolutionary state. For the SoS to function, its constituent systems must be integrated to achieve physical connectivity, and interoperability at all levels, including physical, logical, semantic, and syntactic interoperability. Interoperability allows the necessary connectivity across the SoS to be defined. The boundary of any SoS can be relatively ambiguous because of the dynamic operational focus, multi-mission, and often ad hoc nature of the operational environment of the SoS. In this type of environment, there is a potential for ad hoc coupling across both organizational and systems boundaries in support of the dependencies created. Therefore, in order to use systems successfully, in a SoS context, the protocols used to support the specification of interfaces should be ubiquitous. The interfaces are key convergence points for SoS, and there may be no opportunity for changes to the interfaces without major impact to the entire SoS. The development and management of a SoS architecture through the evolution of a SoS is the mechanism used to document and share information among constituent systems to support integration (ODUSD 2008).

Understanding the constituent system characteristics, functionality, and interfaces is essential to integrating systems into a SoS. Some constituent systems may have interfaces that are changeable without major impact, but others may be prohibitively expensive to modify or may be based on an existing standard2. It is possible that many interfaces are not well-defined or potentially conflicting with other systems (DeLaurentis 2004). Hence SoSE must address the interfaces and interactions of systems during integration. Other than stressing the importance of diligence, little guidance is currently available for any one successful process.

8.1.6 References

Appendix A: Special Considerations for a System of Systems

Reference Code	Reference Source
Ackoff 1971	Ackoff, R.L. “Towards a System of Systems Concept.” *Manag. Sci.* 17, 661-671 (1971).
Baldwin 2009	Baldwin, W.C. & Sauser, B. “Modeling the Characteristics of System of Systems.” *2009 IEEE International Conference on System of Systems Engineering (SoSE)* (2009).
Baldwin 2011-A	Baldwin, W.C., Felder, W.N. & Sauser, B.J. “Taxonomy of Increasingly Complex Systems”. *Int. J. Ind. Syst. Eng.* 9, 298-316 (2011).
Baldwin 2011-B	Baldwin, W.C., Ben-Zvi, T. & Sauser, B.J. “Formation of Collaborative System of Systems through Belonging Choice Mechanisms.” *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans* Early Access, 1-9 (2011).
Biggiero 2001	Biggiero, L. “Sources of Complexity in Human Systems.” *Nonlinear Dynamics, Psychology, and Life Sciences* 5, 3-19 (2001).
Boardman 2006	Boardman, J. & Sauser, B. “System of Systems: The Meaning of *Proceedings of the 2006 IEEE/SMC International Conference on System of Systems Engineering* 118-123 (2006).doi:10.1109/SYSOSE.2006.1652284
Calvano 2004	Calvano, C.N. & John, P. “Systems Engineering in the Age of Complexity.” *Syst. Eng.* 7, 25-34 (2004).
Carlock 1999	Carlock, P.G., Decker, S.C. & Fenton, R.E. “Agency-Level Systems Engineering for “Systems of Systems.” *Systems and Information Technology Review Journal* 7, 99-110 (1999).
Carlock 2001	Carlock, P.G. & Fenton, R.E. “System of Systems (SoS) Enterprise Systems Engineering for Information-Intensive Organizations.” *Systems Engineering* 4, 242-261 (2001).
Carney 2005	Carney, D., Fisher, D. & Place, P. *Topics in Interoperability: System of Systems Evolution*. (Carnegie Mellon University/Software Engineering Institute: Pittsburgh, PA, 2005). http://www.sei.cmu.edu/publications/documents/05.reports/05tn002.html
Checkland 1999	Checkland, P. *Systems Thinking, Systems Practice: Includes a 30-Year Retrospective*. (John Wiley & Sons: Chichester, England, 1999).
Crossley 2004	Crossley, W.A. *System of Systems: An introduction of Purdue University Schools of Engineering’s Signature Area*. (School of Aeronautics and Astronautics, Purdue University: 2004). http://esd.mit.edu/symposium/pdfs/papers/crossley.pdf
Dahmann 2008	Dahmann, J.S., Rebovich Jr, G. & Lane, J.A. “Systems Engineering for Capabilities.” *CrossTalk* 21, 4-9 (2008).

Reference Code	Reference Source
DeLaurentis 2004	DeLaurentis, D.A. & Callaway, R.K." System-of-Systems Perspective for Public Policy Decisions." *Rev. Pol. Res.* 21, 829-837 (2004).
DeLaurentis 2005	DeLaurentis, D.A. & Crossley, W.A. "A Taxonomy-Based Perspective for Systems of Systems Design Methods. *Systems," Man and Cybernetics, 2005 IEEE International Conference on* 1, 86-91 (2005).
Exton 1972	Exton Jr., W. "*The Age of Systems: The Human Dilemma*." (American Management Association, Inc.: United States of America, 1972).
Gideon 2005	Gideon, J.M., Dagli, C.H. & Miller, A. "Taxonomy of Systems-of-Systems." *Proceedings CSER 2005* (2005).
Gorod 2008	Gorod, A., Sauser, B. & Boardman, J. "System-of-Systems Engineering Management: A Review of Modern History and a Path Forward." *IEEE Syst. J.* 2, 484-499 (2008).
INCOSE 2010	*INCOSE Systems Engineering Handbook: A Guide for System Lifecycle Processes and Activities*. Ed. Cecilia Haskins. 3.2 ed. INCOSE-TP-2003-002-03.2. Seattle, WA: International Council on Systems Engineering. 2010.
Kang 2005	Kang, T. & Mavris, D.N. "*A System-of-Systems Approach for Application to Large-Scale Transportation Problems*." 2005 http://www.incose.org/practice/techactivities/wg/sysarch/
Kotov 1997	Kotov, V. *Systems-of-systems as Communicating Structures*. (Hewlett Packard Computer Systems Laboratory: 1997).
Krygiel 1999	Krygiel, A. *Behind the Wizard's Curtain*. (Institute for National Strategic Studies: Washington, DC, 1999) http://www.dodccrp.org/html4/books_downloads.html
Maier 1998	Maier, M.W. "Architecting Principles for System-of-Systems." *Syst. Eng.* 1, 267-284 (1998).
Manthorpe 1996	Manthorpe, W.H.J. "The Emerging Joint System-of-Systems: A Systems Engineering Challenge and Opportunity for APL." *Johns Hopkins APL Technical Digest* 17, 305-310 (1996).
ODUSD 2008	ODUSD(A&T)SSE *Systems Engineering Guide for Systems of Systems*. (Office of the Deputy Under Secretary of Defense for Acquisition and Technology: Washington, DC, 2008). http://www.acq.osd.mil/sse/docs/SE-Guide-for-SoS.pdf
Phillips 1972	Phillips, D.C. "The Methodological Basis of Systems Theory." *Academy of Management Journal* 15, 469-477 (1972).
Schelling 1978	Schelling, T. *Micromotives and Macrobehavior*. (W.W. Norton & Co.: New York, 1978).
Shenhar 1997	Shenhar, A.J. & Bonen, Z. "The New Taxonomy of Systems: Toward an Adaptive Systems Engineering Framework." *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans* 27, 137-145 (1997).

Reference Code	Reference Source
Shenhar 2001	Shenhar, A.J. “One Size Does Not Fit All Projects: Exploring Classical Contingency Domains.” *Manag. Sci.* 47, 394-414 (2001).
Shenhar 2009	Shenhar, A.J. & Sauser, B. “Systems Engineering Management: The Multidisciplinary Discipline.” *Handbook of Systems Engineering and Management* 117-154 (2009).
von Bertalanffy 1950	von Bertalanffy, L. “An Outline of General Systems Theory.” *British Journal for the Philosophy of Science* 1, 139-164 (1950).

8.2 Appendix B: Integrated Technical Management Details

8.2.1 Integrated Technical Management

Planning provides the basis for effective action and the ability to anticipate and prepare for changes that inevitably affect program progress. Planning keeps all organization elements moving synchronously toward the same goal by establishing baseline expectations of future and current actions. By establishing these baselines, the organization is better equipped to adapt to the inevitable changes it faces. Planning specifies the tasks, products, responsibilities, and schedule for managing requirements throughout product development.

All System Engineering (SE) planning shall be included in the System Engineering Management Plan (SEMP) or in a separate standalone plan (e.g., RIO mitigation plan), which ensures a more accurate costing of the program and significantly aids in successful program completion. The SEMP is the only implementing document that integrates all SE activities. It unambiguously ties together all elements of SE required to attain program/project cost, performance, and schedule objectives. The SEMP identifies and ensures control of the overall SE process and provides greater SE implementation detail than the Implementation Strategy and Planning Document (ISPD). Performing these planned activities will significantly reduce the percentage of requirements found in Operational Test and Evaluation. In the Acquisition Management System (AMS), ISPD, details the minimum planning required. The ISPD includes both programmatic and selected SE planning elements. These SE planning elements are summaries of the SEMP planning for same element. The NAS Modernization System Safety Management Plan (SSMP) governs system safety efforts conducted in the AMS and requires each program to develop, as part of the ISPD, an Integrated System Safety Program tailored to the program's safety needs. The AMS also requires the Concept and Requirements Definition plan that addresses a priority service need within the Service Level Mission Need and develops the information necessary for an Investment Analysis Readiness Decision (IARD).

8.2.1.1 Implementation Strategy and Planning Document (ISPD)

The ISPD is the primary document within the AMS for planning the actions and activities to execute the program within the cost, schedule, benefits, and performance baselines. The initial ISPD is required for the Initial Investment Decision (IID) milestone. The initial ISPD contains only the following sections: Overview, Acquisition Plan and Contract Management, Systems Engineering and Development, Physical and Functional Integration, Maintenance Staffing and Planning, and System Safety Management. Information in the initial ISPD is a comparative analysis of alternatives for each of these sections.

A final ISPD is approved at the Final Investment Decision. The final ISPD is the overall implementation plan for the alternative selected for implementation at the IID. The ISPD is reviewed and updated at all subsequent SE and acquisition reviews and reflects changes throughout the program's lifecycle. The ISPD template may be found on FAST, and is summarized in Table 35.

Table 35: Implementation Strategy and Planning Document (ISPD) Table of Contents

1	OVERVIEW
1.1	Mission Need
1.2	Description
1.3	Key Elements
1.4	Use of Contracting

1.5	Key Outputs and Outcomes
2	ACQUISITION PLAN AND CONTRACT MANAGEMENT
2.1	Purpose of Contract(s)
2.2	Sources
2.3	Competition
2.4	Contract Type and Incentives
2.5	Source Selection
2.6	Government-Furnished Property and Information
2.7	Warranties and Data Rights
2.8	Contract Management
2.9	Quality Assurance
3	PROGRAM MANAGEMENT AND CONTROL
3.1	Program Management
3.2	Program Control
4	SYSTEMS ENGINEERING AND DEVELOPMENT
4.1	System Engineering
4.1.1	Hardware and Software Approach
4.1.2	Reliability, Maintainability, & Availability Approach
4.1.3	Configuration Management
4.1.4	Human Factors Approach
4.1.5	Specialty Engineering Approach
4.2	Development
5	PHYSICAL AND FUNCTIONAL INTEGRATION
5.1	Physical Space and Integration
5.2	Integration with other NAS and non-NAS System Elements
5.3	Real Property
5.4	Environmental Requirements
5.5	Hazardous Materials
5.6	Telecommunications

5.7	Spectrum Management
5.8	Information Interoperability
6	MAINTENANCE, STAFFING AND TRAINING
6.1	Maintenance Philosophy
6.2	Staffing
6.3	Training
6.4	Technical Data
7	SAFETY AND HEALTH
7.1	System Safety Management
7.2	Employee Health and Safety
8	SECURITY AND PRIVACY
8.1	Physical Security
8.2	Information Security (See SEM 4.8.6)
8.3	Personnel Security
8.4	Privacy
9	TEST AND EVALUATION
9.1	Test Strategy Overview
9.2	Independent Operational Assessment (IOA)
10	PRODUCTION AND DEPLOYMENT
10.1	Production
10.2	Deployment

8.2.2 SE Planning

For various programmatic reasons, SEMP elements may require a more detailed standalone plan (e.g., RIO mitigation plan). A key function of any plan is to define the tasks and products of the process and to assign responsibilities to various sub-processes. Another key function is to describe the deliverables and portray the schedule for completion of each task and delivery of each product. The details for an individual standalone plan for any SE element are described below. Planning begins in Service Analysis & Strategic Planning, with planning documents baselined at the Final Investment Analysis Decision and updated as necessary.

8.2.2.1 Introduction to the SEMP

As mentioned, the SEMP unambiguously ties together all SE elements required to attain program/project cost, performance, and schedule objectives. It identifies and ensures control of

the overall SE process and provides greater SE implementation detail than the ISPD. SEMP development begins in Service Analysis & Strategic Planning, with the preliminary issue of the SEMP typically occurring in the first phase of Investment Analysis, and a completed version released for Final Investment Decision. A scheduled update occurs in Solution Implementation, with additional updates issued as necessary to reflect changing input conditions throughout the program/project.

8.2.2.2 SE Plan Outputs

Each plan must describe the tasks that reflect the processes detailed in the appropriate SEM section relating to that SE element. This includes a definition of the products and responsibility for the various subprocesses of that element, as well as a task completion schedule. Also, the plan shall detail justification and deviations from the SE element process. Since a key function of the planning is to assign responsibilities to various tasks within the SE element process, one must ensure that each task (in Table E-2) is assigned to a specific individual. These assignments may vary greatly according to the product and the organization. The planning function shall provide a schedule of the SE element (e.g., Architectural Design Synthesis tasks). It is recommended that the schedule show the delivery dates of each product. The schedule presents the sequence of events, along with task start dates and end dates, and keys them to the events outlined in the ISPD template (http://fast.faa.gov). Also, it is recommended that the plan reflect the principles in government and industry standards, such as MIL-STD-961 or MIL-STD-490 for specifications, and EIA 632 for the SE process.

The primary planning tool is a word-processing tool. While the primary metric of the planning process is publication of the plan on schedule, any other metrics selected will also be described in the plan.

Table 36: Contents of the Separate SE Element Plan

SE Element (SEM Section)	What the Standalone SE Plan Contains
Requirements Analysis (Session 3.3)	The plan details the total effort in managing requirements, which includes identifying and capturing requirements, analyzing and decomposing requirements, and allocating requirements (subsection 3.3.2). The other two subprocesses related to Requirements Analysis—Develop Verification Approach and Analyze Verification Data—are the subjects of the Verification and Validation Process in Section 4.7.

SE Element (SEM Section)	What the Standalone SE Plan Contains
Functional Analysis (Section 3.2)	This plan specifies the tasks, products, responsibilities, and schedule for functional analysis throughout development of the product. Because there is no program-level SEMP in the early phases of the program (i.e., phase 1 of Investment Analysis), the NAS-level SEMP guides the Functional Analysis in these phases. When the ISPD is developed, the program's tailored SEMP guides the Functional Analyses. The planning section is baselined at the Final Investment Decision and is updated as necessary at subsequent exit reviews. This planning section details the total effort for managing functional analysis. This work includes analyzing the concept of operations and environment, decomposing functions into subfunctions, decomposing and allocating requirements to functions, evaluating alternative decompositions, defining functional sequences and timelines, defining functional interfaces, and documenting the functional baseline. One must plan for the tasks necessary to develop each Functional Analysis product. The tasks include the following: Define the operational mission, environment, and requirements Develop the Concept of Operations (Use) Define top-level functions and decompose to the lowest level Define internal and external interfaces Evaluate alternative decompositions Develop sequences and timelines Develop functional architecture
Architectural Design Synthesis (Section 3.4)	Architectural Design Synthesis planning includes all activities for transforming the needs into alternative solutions balanced to meet and provide needed capabilities while adhering to programmatic, operational, environmental, and technical constraints. One must plan for the tasks needed to develop each Architectural Design Synthesis product. These tasks include the following: Review the requirements baseline and functional architecture: Design the Solution Set Identify alternatives for the Design Solution Set – Perform Trade Study requests – Initiate Requirements feedback loop – Initiate design feedback loop Allocate requirements to system elements Define design and performance characteristics Define physical architecture Design alternative analysis and refinement Check Requirements compliance Select Preferred Design Solution

SE Element (SEM Section)	What the Standalone SE Plan Contains
Decision Analysis (Section 4.6)	The plan documents the formal management planning regarding how to assess in a fair and impartial manner alternative solutions to a problem or design issue associated with a program/project product development. Decision Analysis planning shall include the following: Formats for how results and information are to be presented to management at design reviews Identification of the organization or person designated to be the decision leader Identification of any tools that are to be used in performing decision (i.e., cost models, computer simulations, test articles and fixtures, and analytical tools) Criteria (including constraints) under which the decision analysis is to be conducted Instructions on where results and data are to be stored for future reference, and which organization is responsible for maintaining the data Identification of resources
Interface Management (Section 4.2)	This plan documents the formal management system of interface controls that ensures physical and functional compatibility between interfacing hardware, software, and facilities. The plan provides the means for identifying and resolving interface incompatibilities and for determining the impact of interface design changes. It guides management, control, and documentation of all system functional and physical interfaces. The Interface Control planning section also contains interface requirements and templates for preparing, revising, and processing ICDs unique to the program. The Interface Control planning section addresses supplier participation in the interface process. The section: Provides the means for identifying, defining, documenting, and controlling the interfaces at all system levels Provides the means for changing the interfaces as required by the evolution of the design and for resolving interface incompatibilities Guides management, control, and documentation of all system functional and physical interfaces Establishes the Interface Working Group (IWG) and its policies and procedures Appoints the IWG chairperson, who also functions as planning coordinator and is responsible for developing and establishing the policies and process for identifying, defining, documenting, auditing, and controlling interfaces Contains requirements and templates for preparing, revising, and processing the interface documentation; identifies products Establishes the participants of the interface management process and their responsibilities Establishes the interface management schedule

SE Element (SEM Section)	What the Standalone SE Plan Contains
Specialty Engineering (Section 5)	The Reliability, Maintainability and Availability (RMA) plan covers all aspects of RMA (see Section 5.1). The Electromagnetic Environmental Effects (E3) plan covers all aspects of E3 (see Section 5.3). The Human Factors Engineering (HFE) plan covers all aspects of HFE (see Section 5.4 and FAA Acquisition System Toolsets). The Quality Engineering (QE) plan covers all aspects of QE. This includes all the systematic activities implemented within the quality system that can be demonstrated to provide confidence that a product or service will fulfill requirements. The Information Security Engineering plan covers all aspects of Information Security (see Section 5.5). Safety (Section 5.6) — Refer to the NAS Modernization SSMP (http://fast.faa.gov/) The Hazardous Materials Management/Environmental Engineering (HMM/EE) plan covers all aspects of HMM/EE (see Section 0).
Risk Management (Section 4.3)	The plan describes the approach, methods, procedures, and criteria for RIO Management and its integration into the program decision process. It is continually updated throughout the program life.
Configuration Management (Section 4.4)	The plan documents the formal Configuration Management (CM) management system to ensure that the integrity and continuity of the design, engineering, and cost tradeoff decisions made among technical performance, producibility, operability, testability, and supportability are recorded, communicated, and controlled by program and functional managers. CM planning enables the following processes: Configuration Identification process that identifies the functional and physical characteristics of selected system components, designated as configuration items (CI), during the system's acquisition lifecycle Configuration Control process that controls the changes to CIs during the system's acquisition lifecycle Configuration Status Accounting process that records/reports change processing and implementation status Configuration Audits process that supplies current descriptions of developing hardware configuration items (HWCIs), computer software configuration items, and the system itself
Verification and Validation (Section 4.7)	The plan describes the overall verification program and provides the content and depth of detail for full visibility of all verification activities. The plan describes and defines each major verification activity. The plan provides a general schedule and sequence of events for major verification activities. It also describes test software (including code and documentation), ground support equipment, and facilities to support verification activities. The systems engineer and verification engineer develop the plan with design and test organizations, with all having a thorough understanding of the verification program concept, program requirements at all levels, and the methods identified in the Verification Requirements Traceability Matrix (VRTM) for verification.
Life Cycle Engineering (Section 5.2)	The plan ensures that resources are available for all activities required for achievement of integrated lifecycle support. Integrated Lifecycle planning includes integrated logistics support, deployment and transition, real property management, sustainment and technology evolution, and disposal.

8.2.3 Inputs to SE Element Plan

Each SE element in Table 37 below has different required inputs. The maturity of these inputs reflects the maturity of the program.

8.2.4 SE Planning Steps

The steps for an individual plan are the same as for the SEMP (see Section 4.1: Integrated Technical Management).

8.2.5 SE Plan Inputs

The table contains the inputs for standalone plans.

Table 37: SE Element Plan Inputs

SE Element	SE Plan Inputs
Requirements Analysis (Session 3.3)	Internal and external requirements as defined in Requirements Analysis Component-specific program guidelines Program-specific organizational constraints and assumptions to be used in the program Program-specific schedule constraints and events Top-level conceptual alternatives, functional analyses, design support alternatives, and initial system evaluations Technology availability or constraints
Functional Analysis (Section 3.2)	Shortfall analysis and final Program Requirements (fPR), which detail the system's expected operational environments Component-specific program guidelines Program-specific constraints and assumptions, such as nature of the program's project teams Program-specific schedule constraints and events NAS SEMP, which provides the overall plan for conducting SE as part of NAS modernization
Architectural Design Synthesis (Section 3.4)	Shortfall analysis and fPR, which detail the system's expected operational environments Component-specific program guidelines Program-specific constraints and assumptions, such as nature of the program's project teams Program-specific schedule constraints and events NAS SEMP, which provides the overall plan for conducting SE as part of NAS modernization
Decision Analysis (Section 4.6)	Definition of the problem to be studied Program/project schedule Program/project requirements Document preparation tools

SE Element	SE Plan Inputs
Interface Management (Section 4.2)	ISPD. This is required to enable preparation of the interface management schedule and to ensure coherent, complete, consistent, and timely interface design at all levels of the system. The SEMP. The IM planning section depends on products defined and scheduled by the SEMP. System Requirements Documents. The documents define the system external interfaces and the (internal) interfaces between the system segments. System Functional and Physical Architecture. These architectures determine where the system/segment interfaces exist and are the point of departure for the detailed identification and definition of the interfaces. Design Review Plans. These plans are used as the bases for conducting reviews and audits of the interfaces (see Section 3.4: Architectural Design Synthesis).
Specialty Engineering (Section 5)	Detailed in Sections 5 through 0.
Risk Management (Section 4.3)	Program goals Program constraints ISPD/Integrated Master Schedule (IMS) Rough Order Magnitude/Basis of Estimate
Configuration Management (Section 4.4)	Concepts (initial, baseline). This data identifies the functional and physical characteristics of selected system components and CIs to be controlled and managed. Data Management plan. Implementation Strategy and Planning Requirements. This data identifies contractual and non-contractual constraints, such as program deliverables, cost, and schedule.
Verification and Validation (Section 4.7)	System ConOps SEMP Final Program Requirements System Physical and Functional Architectures

8.2.6 SE Plan Metrics

The metrics for the standalone plans are in Table 38.

Table 38: SE Element Plan Metrics

SE Element	Recommended Planning Metrics
Requirements Analysis (Session 3.3)	Number of requirements, including stakeholder-specified and project-derived requirements Number of changed requirements, including stakeholder- or project-initiated requirements Technology requirements, including proven, to be defined, and unknown technology requirements Unclear, undefined, or ambiguous requirements Cycle time from requirement change initiation to decision Cycle time from change decision to baseline incorporation Percent of validated requirements to total proposed requirements
Functional Analysis (Section 3.2)	Percent of analysis studies completed (schedule/progress) Depth of the functional hierarchy as a percentage versus the target depth Percent of performance requirements allocated at the lowest level of the functional hierarchy
Architectural Design Synthesis (Section 3.4)	For approved engineering change reports: – Quantity, by type of problem report – Cycle time from disposition to incorporation of change into released engineering documents, by type of report Technical Performance Measurements: objective versus achieved values Number of approved engineering changes by product, type, and stage Documents/drawings submitted for engineering release: – Unacceptable submittals – Total submittals Number of technical action items identified during reviews and audits Design efficiency metrics, such as weight, required power, and envelope dimensions (volume) Cost and schedule variance for completion of Synthesis steps System requirements not met Number or percent of system requirements verified by system analyses Number of TBDs (to be determined) in system architecture or design Number of interface issues not resolved Percent of identified system elements that have been defined
Decision Analysis (Section 4.6)	Cost to produce and update the plan Decision Satisfaction Assessment

SE Element	Recommended Planning Metrics
Interface Management (Section 4.2)	Time from pPR to Interface Requirements Document (IRD) approval Time from IRD Approval to Interface Control document (ICD) Release ICD/Interface Requirement Compliance with Interface Requirements (% "Yes")
Specialty Engineering (Section 5)	Completion of plan Schedule and Progress Resources and Cost Process Performance Customer Satisfaction Product Quality
Risk Management (Section 4.3)	RIO Management can be tracked in three distinct categories: • Board management – board meetings held per the published schedule, and attendance • Training – tracking managers and board members who have taken formal RIO training • Record management – metrics concerning RIO management activity and timeliness of action. Examples of this include: Total RIOs identified over time; total high RIOs, total medium RIOs (to provide visibility into RIO trends over time) Percent of RIOs (medium and high) with approved mitigation plans (to measure effectiveness of handling the RIOs requiring action) Percent of overdue mitigation activities (to measure the effectiveness of meeting mitigation plan schedules) Aging of active RIO records (to gain insight into the timeliness of the RIO database) Number of RIOs past their realization date (to provide an indicator of the effectiveness to handle RIOs in a timely manner)
Configuration Management (Section 4.4)	Metrics criteria for CM should be associated with each CM process task. Example: CM planning: CM plan development milestones Quality completeness Adherence to the plan
Verification and Validation (Section 4.7)	Percent of requirements validated Percent of requirements verified Timeliness of developing and reviewing the verification plan Quality of developing the verification plan Cycle time to complete development and distribution of the verification plan regarding collecting and reviewing the inputs for verification plan development

8.2.7 Requirement Management Planning

Table 39, below, shows the table of contents for a separate Requirements Management Plan if needed. However, this planning is almost always in the SEMP.

Table 39: Table of Contents for Requirements Management Plan

Requirements Management Plan Template		
1	SCOPE	
1.1	Overview	
1.2	Process Overview	Contains a diagram showing the interrelationships among the various process elements, including the requirements management tool, if any.
2	APPLICABLE DOCUMENTS	
3	TASKS	Describes the tasks that are tied to the specific organizational and program requirements in accordance with Section □.
3.1	Identify and Capture Requirements	
3.2	Analyze and Decompose Requirements	
3.3	Allocate Requirements	
3.4	Derive Requirements	
3.5	Manage Requirements Changes	
4	PRODUCTS	Describes the various program requirements documents. It also describes what organizational entity receives the product. For example, the product team, stakeholder, other project teams, management, or outside organizations, such as manufacturing, product support, test and evaluation, or supplier management.
4.1	Requirements Documents	Enumerates and describes the various program requirements documents to be produced.
4.2	Requirements Allocation Matrices	Describes the characteristics of the requirements allocation sheets to be produced on this program.
5	RESPONSIBILITIES	Details responsibilities of the various organizational entities to accomplish the tasks of Section 3 above. The responsibilities are to be tied to the tasks of Section 3.
6	SCHEDULE	Contains schedule that is tied to the milestones of the ISPD.
7	AUTOMATED REQUIREMENTS TOOL	Describes the planned use of the requirements management tool, if available.
8	NOTES	
	APPENDICES	

8.2.8 Functional Analysis Planning

Table 40, below, presents the table of contents used if it is determined a separate Functional Analysis Plan is needed. However, this planning is almost always in the SEMP.

Table 40: Table of Contents for Functional Analysis Plan

Functional Analysis Plan Template		
1	SCOPE	
1.1	Overview	
1.2	Process Overview	Contains a diagram showing the interrelationship among the various process elements, including tools, if any.
2	APPLICABLE DOCUMENTS	
3	TASKS	Describes the tasks that are tied to the specific organizational and program requirements in accordance with Section 3.2.
4	PRODUCTS	Describes the various Functional Analysis outputs. Also describes what organizational entity receives the product. For example, the product team, stakeholder, other project teams, management, or outside organizations, such as manufacturing, product support, test and evaluation, or supplier management.
5	RESPONSIBILITIES	Details responsibilities of the various organizational entities to accomplish the tasks of Section 3. The responsibilities are to be tied to the tasks of Section 3.
6	SCHEDULE	Contains the schedule that is to be tied to the milestones of the ISPD.
7	AUTOMATED REQUIREMENTS TOOL	Describes the planned use of the requirements management tool, if any.
8	NOTES	
	APPENDICES	

8.2.9 Architectural Design Synthesis Planning

Table 41, below, provides the table of contents used if it is determined a separate Architectural Design Synthesis Plan is needed. However, this planning is almost always in the SEMP.

Table of Contents of for Architectural Design Synthesis Plan

Table 41: Table of Contents of for Architectural Design Synthesis Plan

Architectural Design Synthesis Planning Section Template		
1	SCOPE	
1.1	Overview	

Architectural Design Synthesis Planning Section Template		
1.2	Process Overview	Contains a diagram showing the interrelationships among the various process elements, including tools, if any.
2	APPLICABLE DOCUMENTS	
3	TASKS	Describes the tasks that are tied to the specific organizational and program requirements in accordance with Section 3.4.
4	PRODUCTS	Describes the various Architectural Design Synthesis outputs in accordance with Section 3.4 as well as what SE element receives the product.
5	RESPONSIBILITIES	Details responsibilities of the various organizational entities to accomplish the tasks of Section 3. The responsibilities are to be tied to the tasks of Section 3.4.
6	SCHEDULE	Contains the schedule that is to be tied to the milestones of the ISPD.
7	AUTOMATED REQUIREMENTS TOOL	Describes the planned use of the requirements management tool, if any.
8	NOTES	
	APPENDICES	

8.2.10 Decision Analysis Planning

Table 42, below, features the table of contents used if it is determined a separate Decision Analysis Plan is needed. However, this planning is nearly always in the SEMP.

Table 42: Table of Contents for Decision Analysis Plan

Decision Analysis Plan Template		
1	SCOPE	
1.1	Overview	
1.2	Process Overview	Contains a diagram showing the interrelationships among the various process elements, including tools, if any.
2	APPLICABLE DOCUMENTS	
3	TASKS	Describes the tasks that are tied to the specific organizational and program requirements in accordance with Section 4.6.
4	PRODUCTS	Describes the output of Decision Analysis activities.
5	RESPONSIBILITIES	Details responsibilities of the various organizational entities to accomplish the tasks of associated with Decision Analysis.
6	SCHEDULE	Contains the schedule that is to be tied to SEMP milestones.

Decision Analysis Plan Template		
7	AUTOMATED REQUIREMENTS TOOL	Describes the planned use of tools.
8	NOTES	
	APPENDICES	

8.2.11 Interface Management Planning

Table 43, below, lists the table of contents for a separate Interface Management Plan if needed. Interface Management is frequently a separate plan.

Table 43: Interface Management Plan Outline

Interface Management Plan Outline	
1	SCOPE
1.1	Overview
1.2	System Overview
2	APPLICABLE DOCUMENTS
3	INTERFACE WORKING GROUP
3.1	IWG Policy and Procedures
3.2	IWG Membership and Responsibilities
3.2.1	IWG Chair
3.2.2	Interface Custodian
3.2.3	Interface Participant
4	INTERFACE CONTROL PROCESS
4.1	Establishing Interfaces
4.1.1	Identifying Interfaces
4.1.1.1	Scope Sheet
4.1.1.2	Documenting ICDs
4.1.1.3	Coordinating Interfaces
4.1.1.4	Auditing, Statusing, and Controlling ICDs
4.1.1.4.1	Authorized ICD List
4.1.1.4.2	Review at SRR

Interface Management Plan Outline	
4.1.1.4.3	Review at SDR
4.1.1.4.4	Review at Preliminary Design Review (PDR)
4.1.1.4.5	Review at CDR
4.1.1.4.6	Review at FCA/PCA
5	REVISING INTERFACES
5.1	Change Request Preparation
5.1.1	Review/Coordinate Change Request
5.1.2	Change Approval and Documentation
6	INTERFACE MANAGEMENT SCHEDULE
7	NOTES
Appendices	

8.2.12 RIO Management Planning

RIO is inherent in every program. Stakeholders know this and expect contractors to address RIOs in program plans. SE addresses three facets of RIO: technical, schedule, and cost. Technical RIOs include all events that may prevent the program from satisfying contractual requirements, including performance, supportability, maintainability, and regulatory requirements. Schedule RIOs are events that may prevent timely execution of tasks identified in the ISPD. Cost RIOs are events that may cause actual expenditures to exceed estimated costs.

RIO management is a key process within SE. The program and functional managers implement it by ensuring that appropriate resources are applied to reduce RIO to acceptable levels. RIO management consists of five essential components: identify RIOs, analyze RIOs, identify mitigation options, implement the RIO-reduction plan, and monitor RIOs.

The RIO Management planning section describes the approach, methods, procedures, and criteria for RIO management and its integration into the program decision process. It is continually updated throughout the program life with the SEMP.

8.2.12.1 RIO Management Planning Outputs

Table 44, below, is a template that may be used for the RIO Management Plan.

Table 44: Table of Contents for RIO Management Plan

Risk Management Planning Section Outline	
1	Introduction – Purpose, Scope, Document Organization
2	RIO Management Process – Definitions, Step 1, Step 2, …, Status Options
3	RIO Management Meetings – RMB, Manager Status Meetings, Meeting Frequency
4	RIO Tools

Risk Management Planning Section Outline	
5	Roles and Responsibilities
6	Process Health Metrics
7	Process Improvement and Training
8	Requirements
9	Safety and Security Risk Coordination
	Appendices – Board Structure, References, Meeting Agendas, RIO Sources, Scorecards, etc.

8.2.13 Configuration Management Planning

The Configuration Management Organization typically owns this planning section. Inputs from the SE process may initiate the planning section as early as the Investment Analysis, phase one, but the section formally starts at Investment Analysis, phase two, and continues throughout the program lifecycle as the system develops and is modified.

8.2.13.1 Outputs of Configuration Management Planning

The output shall be the Configuration Management planning section of the SEMP that outlines all the tasks with corresponding completion dates and personnel responsible for task completion or a standalone plan containing the same information as the Table 45 template.

Table 45: Table of Contents for Configuration Management Plan

Configuration Management Plan Outline	
1	SCOPE
1.1	Overview
1.2	System Overview
2	CONFIGURATION MANAGEMENT REVIEW TEAM
3	CONFIGURATION MANAGEMENT PROCESS
3.1	Process
3.2	CONFIGURATION MANAGEMENT Assessment Criteria and Mitigation Requirements
3.3	Key Decision Points
3.4	Documentation Requirements
4	CONFIGURATION MANAGEMENT MONITORING PROCEDURE
5	CONFIGURATION MANAGEMENT SCHEDULE
6	Data Management Planning

Configuration Management Plan Outline	
7	NOTES AND REFERENCES
8	APPENDICES
8.1	Documentation Forms
8.2	CONFIGURATION Management Tools

8.2.14 Concept and Requirements Planning

The Concept and Requirements Plan (see Table 46 template below) specifies the scope, assumptions, constraints, methods, data sources, resources, control strategy, team composition, roles and responsibilities, schedule, and deliverables for a proposed concept and requirements definition (CRD) activity. The CRD addresses a priority service need within the Service Level Mission Need Statement and develops the information for an investment analysis readiness decision (IARD).

Table 46: Table of Contents for Concept and Requirements Plan

Concept and Requirements Plan Template		
1	SCOPE	
1.1	Service Level Mission Need	Identifies the specific capabilities or components of the Service Level Shortfall Analysis that will be examined.
1.2	Service Delivery Strategy	Defines how these capabilities or components fit into the overall service delivery strategy of your service organization.
1.3	Assumptions, Constraints, and Guidance	States the key assumptions, constraints, and guidance that will govern the CRD Team as it conducts CRD activities. These *may* include: The quantified capability shortfall that will be addressed The remaining service life of the existing capability The required operational date of any needed new or replacement capability Any component of the proposed new capability that has a higher priority for early delivery than the entire capability The required mission life or economic service life of the proposed new capability The proposed date for the IARD—date by which all CRD activity must be complete with findings and recommendations presented to the appropriate decision board (Executive Council (EC) for Air Traffic Organization (ATO); Information Technology Executive Board (ITEB), which reviews and recommends investments related to FAA administrative and some mission support services; and the lines of business (LOB) review boards that review and recommend investments within a LOB Any design cost, unit acquisition cost, Operations cost, or any other economic goal that must be satisfied by the new or replacement capability (e.g., “Unit initial acquisition cost must be less than $2 Million.”) Any ATO/LOB performance goal that must be satisfied by the new or

Concept and Requirements Plan Template		
		replacement capability (e.g., “Reduce cost per flight by 1%.”) Any milestone constraint (i.e., external influences) that must be satisfied by the new or replacement capability Any constraints on the choice of an alternative (e.g., “No alternative may be developed that will require the mandatory carriage of new avionics by the airlines and other National Airspace System (NAS) users.”) Any policy guidance that influences, constrains, or dictates the choice of a new or replacement capability or operational requirement Any interdependencies with other new, existing, or proposed Federal Aviation Administration assets that must be satisfied (e.g., “Delivery of new digital Airport Surveillance Radar-11 radars must be completed prior to installation of new digital Standard Terminal Automation Replacement Systems.”) Any NAS safety issues that influence, constrain, or dictate the choice of a new or replacement capability Any required safety risk acceptance and safety risk management documentation.
1.	Methodology	Defines the methodologies and techniques to be used in each CRD activity and task.
2	APPLICABLE DOCUMENTS	
3	TASKS	Define tasks necessary to ensure a program is ready for investment analysis.
3.1	Identify Required Resources	Identifies the resources and respective costs needed to complete CRD activities. For example, what team members are needed? What are the required skill levels? What level of effort must they provide (weekly time commitment)? What level of contract support is needed? Are any consultants needed? What travel, training, or technology (software or hardware) is required?
3.1.1	Personnel	Identifies required team member skill. Identify time commitment (level of effort).
3.1.2	Contract Support	Determines what level of contract support is need.
3.1.3	Training	Determines is any unique training is required.
3.1.4	Travel	Determines what, if any, travel is required.
3.1.5	Technology Needs	Determines if any technology (hardware and/or software) is needed to perform CRD process.
3.16	Costs	Determines costs for 3.1.1 through 3.1.5.
3.2	Specify Team Composition	Specifies the CRD Team composition alphabetically by name and affiliated FAA organization. Acquisition Management System policy designates ATO Operations Planning (ATO-P) Systems Engineering as lead.

Concept and Requirements Plan Template		
3.3	Define Data Requirements	Defines the data sources that will be used for each CRD activity.
3.4	Control Strategy	Describes the control strategy that will be used by the CRD Team Lead to ensure timely delivery of quality CRD products to the EC/LOB/ITEB. Discuss how commitment to these activities will be obtained.
3.4.1	Commitment	Establishes a methodology to ensure that personnel are available to meet team commitments. This may be accomplished through a request for participation, memorandum for action or memorandum of understanding, letter of agreement, bargaining negotiations, or management coordination.
4	Deliverables	Lists and describes all CRD deliverables and provides the required completion date for each. At a minimum, CRD deliverables shall include a Preliminary Program Requirements attachment including Preliminary Program Requirements, Functional Architecture, and Technical Description; identification of the alternatives that will be evaluated during initial investment analysis, along with a rough estimate of lifecycle cost for each alternative; an assessment of the alternatives against the Enterprise and Security Architectures; an Operational Safety Assessment; Safety Risk Management Decision Memo; and Initial Investment Analysis Plan.
4.1	System Engineering	Enumerates and describes the various system engineering analyses and documents to be produced.
4.2	Cost	Enumerates and describes the various cost analyses and documents to be produced.
4.3	Briefings	Discusses the briefings as well as the associated content, format, and scheduling criteria.
5	RESPONSIBILITIES	Defines the roles and responsibilities of each team member for each CRD activity and deliverable; also defines who will prepare CRD briefing and who will be responsible for briefing the EC.
	Develop WBS	Develops a work breakdown structure and matched organizational breakdown structure for all CRD activities and deliverables.
6	SCHEDULE	Provides schedules and an integrated network for conducting all CRD activities and completing required deliverables. The schedule should show start, duration, and completion of all major CRD activities. The integrated schedule should, at a minimum, identify such things as activity dependencies and interdependencies, slack times, and the critical path for project completion.
7	AUTOMATED REQUIREMENTS TOOL	Describes the planned use of the requirements management tool, if any.
8	NOTES	
	APPENDICES	

8.2.15 Verification Planning

8.2.15.1 Verification Plan

The Verification Plan describes the overall verification program. It provides the content and depth of detail for full visibility of all verification activities and fully describes each major verification activity. The plan provides a general schedule and sequence of events for major verification activities. It also describes test software (including code and documentation), Ground Support Equipment, and facilities to support verification activities. The systems engineer and verification engineer develop the plan with design and test organizations, with all having a thorough understanding of the verification program concept, program requirements at all levels, and the methods in the Verification Requirements Traceability Matrix (VRTM) for verification.

8.2.15.2 Verification Requirements Traceability Matrix

The VRTM is that portion of a requirements document that defines how each requirement is to be verified. It includes the plan that describes the verification activity as well as the results, including traceability to testing (in the verification report). The VRTM is based on the Validation Table documented in the Validation Report. The design, test, SE, and verification team members jointly develop the VRTM. The VRTM establishes the basis for the verification program.

8.2.15.3 Requirements Verification Compliance Document (RVCD)

The RVCD provides the evidence of compliance for each requirement at all levels and to each VRTM requirement. The flow down from the requirements documents to the VRTM completes the full requirements traceability. Compliance with all requirements ensures that the system-level requirements have been met.

The RVCD defines for each requirement the methods of verification and corresponding compliance information. The results of the verification activity, including evidence of completion, are recorded and documented in the RVCD. It is recommended that the RVCD contain information regarding the results of each verification activity and a description and disposition of conformance, nonconformance, conclusions, and recommendations. The compliance information provides either the actual data or a reference to the location of the actual data that shows compliance with the requirement. The document also includes a section that details any non-compliances; it is recommended that this section also specify appropriate re-verification procedures. The RVCD is an input into the Requirements Management process (Section 3.3). Decisions regarding what to do with noncompliant requirements are made in Requirements Management.

8.2.15.4 Verification Plan Metrics

The Verification Plan provides the content and depth of detail for understanding the Verification activities, detailing each major activity. It contains the schedule and sequence of events. Table 47, below, is a template for the plan.

Table 47: Table of Contents for Verification Plan

Verification Plan Template		
1	SCOPE	
1.1	Overview	
1.2	Process Overview	Contains a diagram showing the interrelationships among the various process elements, including tools, if any.
2	APPLICABLE	

Verification Plan Template		
	DOCUMENTS	
3	TASKS	Describes tasks that are tied to the specific organizational and program requirements in accordance with Section 4.12. Includes qualification, acceptance, predevelopment, operational, and disposal Verification activities for hardware, software, and procedures.
4	PRODUCTS	Describes all associated products (e.g., VRTM and RVCD).
5	RESPONSIBILITIES	Details responsibilities of the various organizational entities to accomplish the Validation and Verification tasks.
6	SCHEDULE	Contains the schedule that is to be tied to the milestones of the SEMP.
7	Validation and Test	Describes the planned test hardware and software, support equipment, and facilities required to support Verification activities.
8	NOTES	
	APPENDICES	

8.2.16 Integrated Human Factors Planning

Table 48 shows the table of contents for a separate integrated human factors plan, if considered necessary by the program.

Table 48: Integrated Human Factors Plan Content and Format

Headings		Content
Background	Program Summary	Briefly describe the program Describe concept of operation and maintenance
	Program Schedule	Provide overview of system acquisition schedule
	Target Population	Identify: Operator and maintainer Demographics Biographical data Previous training Aptitudes Task-related experience Anthropometric data Physical qualifications Organizational relationships Workspace requirements
	Guidance	Summarize any guidance received

Headings		Content
	Constraints	State if additional staffing is required by the new system State whether an existing job series is to be used or a new one created Post limits on the amount of time that may be afforded for training Establish standards on the working conditions that are to be acceptable when the new system is fielded Describe limitations imposed by maintenance policy Develop requirements as a result of union agreements
Issues and Enhancements	Issue Description	Describe the issue or problem background, importance, and consequences or task to be done to support the acquisition
	Objectives	Identify Human Factors Program objectives Provide performance measures and criteria in terms of time and accuracy to perform tasks to evaluate resolution of issue When human performance thresholds are known, identify tasks for the developer to be done early enough in the acquisition to influence requirements and system engineering Identify the actions to be taken to resolve each issue Show the current status of each issue
	Actions	Identify actions to be taken to resolve issues Show current status of each action
Activities	Activity Description	Identify any tasks, studies, or analyses that shall be performed to resolve the issues (e.g., contractor's Human Engineering Program Plan per MIL-HDBK-46855, Functional Analysis to support equipment versus people allocation of functions, Task Analysis to produce a specific operator, and maintainer task list)
	Activity Schedule	By acquisition phase, describe the human factors tasks in terms of who, what, when, and how (resources) Identify feeds to and dependencies on ILS, training, and test and evaluation programs
Strategy	Goals and Requirements	Derive Strategy from the major concerns, issues, schedule, tasks, guidance, constraints, objectives, and approach for the Human Factors Program Answer the question, "What objectives does the government wish to achieve?" Answer the question, "How is the government to accomplish these objectives?"
	Approach	Identify who is to be responsible for the Human Factors Program Set out the extent of contractor support required Define how human factors resources are to be organized and managed to support the system acquisition
	References	Identify relevant references needed for a full understanding of the Human Factors Program

Headings		Content
Review	Review	Identify administrative handling procedures Identify update schedule and procedure Identify review procedures

8.3 Appendix C: System Engineering Technical Reviews and Associated Checklists

8.3.1 Introduction

This appendix and associated Risk checklists are used to support implementation of the System Engineering (SE) Technical Reviews specified in Section 4.1.4: Technical Monitoring and Control. This appendix contains sections on the individual SE Technical Reviews and the technical elements of supporting reviews. These sections describe the purpose, entry criteria, planning, timing, conduct, exit criteria, and completion of each type of SE Technical Review.

The SE Technical Reviews (or milestones) in Section 4.1.4 are integral parts of the FAA SE process and lifecycle management. The FAA Product Development Process, Figure 36, shows the relationship of these milestones with the acquisition phases and decision points. The Technical Reviews provide an independent assessment of the technical progress of the program and highlight areas that corrective action may need to be taken.

> ***Tip**: These reviews are **not the place for problem-solving**, but to verify that the problems are being addressed. They are a risk-reduction approach that manages the progress of the technical aspects of a system development or deployment.*

The contents of this appendix are provided for guidance. Reviews and checklists are intended to be tailored based on program needs and experience. Tailoring or elimination of a specific SE milestone should be coordinated with NAS Systems Engineering (or the non-NAS equivalent) and documented in the program Systems Engineering Management Plan (SEMP). Based on the structure of the program and the AMS entry point, a program may not need to conduct every review. Certain reviews may be performed incrementally by configuration item, especially for complex systems.

8.3.2 System Engineering Milestones and Technical Reviews

Each technical review or audit should establish the readiness of a program to proceed to the next phase of the system's lifecycle. Typically, reviews focus on the development phases, where SE provides the largest benefit to the investment. Reviews and audits are scheduled at strategic points within the development cycle and are usually conducted in conjunction with, or in preparation for, a lifecycle phase milestone at which the decision to advance to the next phase is made. Technical reviews employ specific criteria tailored to each phase of the lifecycle. These criteria verify the extent of technical progress made toward the solution of the identified capabilities shortfall.

The FAA has a set of reviews established to support its system lifecycle model. Section 4.1.4.7 discusses the generic use and structure of Technical Reviews, but it is recognized that this generic construct must be tailored to some extent for each review. This appendix contains the application of the generic review model and details of specific review tailoring along with some best practice techniques and approaches.

At any given SE Technical Review, a chairperson leads the review. The review itself is conducted and approved in accordance with the provisions of the governing SEMP. SE Technical Review approval, as it relates to this appendix, is defined as the following:

34. Approval of the Request(s) For Action (RFA) generated during the review
35. The readiness of the design/development to proceed to the next technical phase of the program
36. Dissemination of the assessment of risk generated during the review

Completion of a Technical Review occurs after all RFA forms have been addressed and assessed, the status agreed upon, an updated Risk Assessment completed, and the review minutes promulgated.

8.3.2.1 Service Analysis and Strategic Planning Phase

Per the FAA AMS, Service Analysis and Strategic Planning is the crucial beginning phase of the lifecycle management process. It determines what capabilities must be in place now and in the future to meet agency goals and the service needs of customers. Results are captured in the "as is" and "to be" states of the enterprise architecture, as well as the roadmaps for moving from the current to the future state. The following SE milestones are associated with the Service Analysis and Strategic Planning phase:

- Technology Readiness Assessment (TRA)

8.3.2.2 Concept and Requirements Definition

All investment opportunities that require funding outside the scope of an approved acquisition program baseline undergo concept and requirements definition. Concept and requirements definition translates priority operational needs in the enterprise architecture into preliminary requirements and a solution concept of operations for the capability needed to improve service delivery. It also quantifies the service shortfall in sufficient detail for the definition of realistic preliminary requirements and the estimation of potential cost and benefits. The following SE milestone is associated with the Concept and Requirements Definition phase:

- Investment Analysis Readiness Decision

8.3.2.3 Investment Analysis Phase

Per the FAA AMS, the Investment Analysis phase of the Acquisition lifecycle is conducted to ensure that the critical needs of the FAA are satisfied by practical and affordable solutions. Initial investment analysis rigorously evaluates alternative solutions to mission need and determines which offers the best value and most benefit to the FAA and its customers within acceptable cost and risk. Final investment analysis develops detailed plans and final requirements for the proposed investment program, including an acquisition program baseline that establishes cost, schedule, performance, benefits, and risk-management boundaries for program execution. The following SE milestones support the effort to obtain a favorable investment decision:

- System Requirements Review (SRR) — Program level

8.3.2.4 Solution Implementation Phase

The Solution Implementation phase of the AMS begins at the final investment decision, when the JRC approves and funds an investment program, establishes its program baseline for variance tracking, and authorizes the Service Organization to proceed with full implementation. Solution implementation ends when a new service or capability is commissioned into operational use. The following SE Technical Reviews support execution of a program during Solution Implementation:

- System Requirements Review (SRR) — Contract level
- System Design Review (SDR)
- System Specification Review (SSR)
- Preliminary Design Review (PDR)
- Critical Design Review (CDR)
- Test Readiness Review (TRR)
- In Service Review (ISR)
- Technology Readiness Assessment (TRA)

8.3.2.5 In-Service Management

Activity during In-Service management supports execution of the FAA mission of providing air traffic control and other services. This includes operating, maintaining, securing, and sustaining systems, products, services, and facilities in real time to provide the level of service required by

users and customers. It also entails periodic monitoring and evaluation of fielded products and services as well as feedback of performance data into Mission and Investment Analysis as the basis for revalidating the need to sustain deployed assets or taking other action to improve service delivery. The following SE Technical Reviews support In-Service Management:

- In-Service Performance Review (ISPR)
- Functional Configuration Audit (FCA)
- Physical Configuration Audit (PCA)
- Production Readiness Review (PRR)

8.3.2.6 Disposal

The AMS states that "Service organizations must remove and dispose of fielded assets and services when they are no longer needed. This includes restoration of sites where obsolete products or services were deployed, government property disposal, precious metals recovery, and cannibalization of useful assets. The cost of removal and restoration is included in the Exhibit 300 Program Baseline of the *replacement program*. If there is no replacement program, the cost must be otherwise factored into the service-area operating plan. Removal and disposal includes decommissioning, dismantling, and demolishing of systems and equipment; restoring sites including environmental cleanup and disposal of hazardous materials; disposing of government property; recovering precious metals; and reusing surplus assets."

There are no SE milestones uniquely associated with the Disposal phase. The SE decision efforts are conducted during earlier phases of the lifecycle.

8.3.3 FAA System Engineering Milestones and Technical Reviews

SE milestones are described in this section — each on its own "fact sheet." These sheets describe the purpose, timing, entry criteria, planning, conduct, exit criteria, completion of each SE milestone (also called a Technical Review), and helpful tips.

Each SE Technical Review has an associated Program Risk Assessment Checklist. These checklists should be used in conjunction with the SEMP during execution of the program. The Risk checklists are living documents, intended to be updated based on user experiences. The checklists are an effective tool for preparing for and conducting a review. Use the following criteria to complete the checklist(s):

- **Green.** The requisite criteria and/or documentation is available and of sufficient quality to conduct the review.
- **Yellow.** The requisite criteria and/or documentation are available and partially suitable to conduct the review.
- **Red.** The requisite criteria and/or documentation are NOT available or not sufficient to conduct the review.

8.3.3.1 Technology Readiness Assessment (TRA)

The TRA is a multi-disciplined technical review that assesses the maturity of Critical Technology Elements (CTE) being considered to address user needs and analyzes operational capabilities and environmental constraints within the Enterprise architectural framework. The TRA validates capability gaps at the NAS (or non-NAS) level to be addressed by the service units or Lines of Business (used to support service unit's initial Shortfall Analysis submission) and determines extent that new and/or novel technologies may be mature enough to be considered to address the gap. If a specific technology or its application is either new or novel, then that technology is considered a CTE. The TRA is not a risk assessment but is a systematic metrics-based tool to identify and allow for early attention to technology maturation events. The TRA will score each identified CTE using 9 Levels of Maturity (LOM) (Table 49) for both hardware and software.

Table 49: LOM Descriptions

LOM	Definition	Description	Supporting Documentation
1	Basic principles observed and reported	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.	Published research that identifies the principles that underlie this technology. References to who, where, when.
2	Technology concept and/or application formulated	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.	Publications or other references that outline the application being considered and that provide analysis to support the concept.
3	Analytical and experimental critical function and/or characteristic proof of concept	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.	Results of laboratory tests performed to measure parameters of interest and comparison to analytical predictions for critical subsystems. References to who, where, and when these tests and comparisons were performed.
4	Component and/or breadboard validation in laboratory environment	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.	System concepts that have been considered and results from laboratory-scale breadboard(s). References to who did this work and when. Provide an estimate of how breadboard hardware and test results differ from the expected system goals.

LOM	Definition	Description	Supporting Documentation
5	Component and/or breadboard validation in relevant environment	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of components.	Results from testing a laboratory breadboard system are integrated with other supporting elements in a simulated operational environment. How does the “relevant environment” differ from the expected operational environment? How do the test results compare with expectations? What problems, if any, were encountered? Was the breadboard system refined to more nearly match the expected system goals?
6	System/subsystem model or prototype demonstration in a relevant environment	A representative model or prototype system, which is well beyond that of LOM 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in a simulated operational environment.	Results from laboratory testing of a prototype system that is near the desired configuration in terms of performance, weight, and volume. How did the test environment differ from the operational environment? Who performed the tests? How did the test compare with expectations? What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before moving to the next level?
7	System prototype demonstration in an operational environment	Prototype near, or at, planned operational system. Represents a major step up from LOM 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space. Examples include testing the prototype in a test bed aircraft.	Results from testing a prototype system in an operational environment. Who performed the tests? How did the test compare with expectations? What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before moving to the next level?

LOM	Definition	Description	Supporting Documentation
8	Actual system completed and qualified through test and demonstration	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this LOM represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.	Results of testing the system in its final configuration under the expected range of environmental conditions in which it will be expected to operate. Assessment of whether it will meet its operational requirements. What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before finalizing the design?
9	Actual system proven through successful mission operations	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.	Operational Test and Evaluation (OT&E) reports.

8.3.3.1.1 Timing and Relationship to AMS

The assessment of new and/or promising technologies occurs at two distinct points in the AMS lifecycle, Product Planning and Development Process: (1) during Service Analysis & Strategic Planning to support a determination of those alternate technologies to be considered during Investment Analysis, and (2) during the In-Service Management phase of the AMS to determine if technology insertion is warranted to address user needs.

Related AMS products:

- Shortfall Analysis
- Standards, guidance, and tools for Service-level Mission Analysis

8.3.3.1.2 Entrance Criteria and Inputs

These include the following:

- Enterprise Architecture
- Concept of Operations
- Concerns and Issues
- Technology
- Market Research
- Need
- Corporate Strategy and Goals
- Legacy System

8.3.3.1.3 Tasks

(Reserved)

8.3.3.1.4 Exit Criteria and Outputs

These include the following:

- Validated NAS Functional portion of Enterprise Architecture
- Technology opportunities
- Updated Risk Assessment
- Gap Analysis

8.3.3.1.5 Metrics

(Reserved)

8.3.3.1.6 Tools

TRA Risk Reduction Checklist (see file 060517 FAA TRA Checklist V31)

8.3.3.2 Functional Baseline Review (FBR)

The FBR is a formal review to ensure that requirements have been completely and properly identified and that there is a mutual understanding between the implementing organization and stakeholders. It validates program cost, schedule, and performance to support Milestone approvals. It captures functional requirements that go with the Mission Analysis and Investment Analysis phases and establishes the functional baseline as the governing technical description, which is required before proceeding to the next AMS phase or Decision gate.

8.3.3.2.1 Timing and Relationship to AMS

It is conducted just before the Initial Investment Decision (AMS Milestone 3).

8.3.3.2.2 Entrance Criteria and Inputs

These include the following:

- (pRD — previously the iRD)
- Constraints
- FAA Policy
- Standards
- Integrated Master Schedule (IMS)
- Investment risks

8.3.3.2.3 Tasks

(Reserved)

8.3.3.2.4 Exit Criteria and Outputs

These include the following:

- Final Requirements Set — (fRD)
- Program Work Breakdown Structure (WBS)
- Program Statement of Work (SOW)
- Final SEMP

8.3.3.2.5 Metrics

(Reserved)

8.3.3.2.6 Tools

FBR Risk Reduction Checklist

8.3.3.3 System Requirements Review (SRR)

The SRR determines whether the System Requirements Document (Type A Specification) correctly and completely represents the operational and constraint requirements defined in the fPR. This review also determines if the proposed functional architecture is consistent with the system requirements. The SRR occurs early in the development process before expenditure of any extensive design definition effort. As part of the process of determining whether the system requirements and architecture capture the mission's needs, values for all TPPs are projected based on system requirements and compared to the target values and critical limits set during investment analysis. The results of the TPM analysis become part of the output of the SRR. Additional TPPs might be added depending on requirement changes approved at the SRR. Critical performance limits might also be adjusted based on approved requirement changes.

- **Program level.** The SRR is a formal internal FAA review to ensure that the system requirements have been completely and properly identified. It validates program cost, schedule, and performance to support Milestone approvals. It assesses the technical readiness of the program to begin implementation and establishes the Allocated baseline as the governing technical description, which is required for the next AMS Acquisition phase.
- **Contract level.** The SRR at the contract level is a formal, system-level review conducted to ensure that system requirements have been completely and properly identified and that a mutual understanding between the government and contractor exists. It assesses the contractor's readiness to begin development.

8.3.3.3.1 Timing and Relationship to AMS

The program SRR is conducted just before the Investment Decision (AMS Investment Milestone 4). The contract SRR is conducted shortly after both AMS Milestone 4 and contract award (prior to the beginning of functional allocation activities) to assess the contractor's readiness to begin development.

8.3.3.3.2 Entrance Criteria and Inputs

Access to the IMS and LCE cost estimate(s) are a prerequisite for conducting a successful SRR. Previously completed products that are required before proceeding to SRR include:

- pPR/fPR
- List of allocated TPPs and associated critical performance limits and target values
- Constraints
- IRDs (draft)
- Risk identification and mitigation plans
- Any proposed changes to the above items as a result of the work leading up to the SRR

Products that are to be submitted for review as part of the SRR include:

- System Requirements Document/Type A Specification (draft)
- System Functional Architecture (draft)
- A report on the results of the TPM analyses
- System specification, SOW, and the contract WBS (included at the contract level SRR).

8.3.3.3.3 Tasks

The following tasks are required to successfully accomplish the SRR (independent of level):

- Define SRR objectives and scope
  - Establish success criteria, prerequisites (entry criteria), and approach to be used
  - Set the date for the SRR and activities leading up to the review

  - Create an agenda for the review
  - Identify and notify participants and stakeholders of their roles and responsibilities
- Identify the item(s) to be reviewed and the extent of review of each
- Compile the SRR-related data package. This package contains the SRR presentation material and all of the pertinent backup material.
- Distribute the SRR documentation to the stakeholder representatives and request timely review responses
- Obtain readiness approval for SRR and comments to the data package made via Review Item Discrepancy submissions
- Incorporate changes in the data package as needed
- Develop a summary of all concerns submitted and their respective answers
- Update risk management plans based on review
- Conduct SRR with the incorporated changes
- Document and publish SRR minutes
- Compile action-item and issues lists
- Track action items and issues
- Document closed action items and distribute to the SRR stakeholders

8.3.3.3.4 Exit Criteria and Outputs

These include the following:

- Approved System Requirements Document/Type A Specification
- Approved System Functional Architecture
- Approved changes to the fPR
- Approved changes to the IRDs
- Approved changes to the TPPs
- Approved TPM report
- Updated Risk Management Plan(s)
- System Specification (includes obtaining contractor agreement at contract SRR)
- Risks for recommended alternative
- LCE cost estimate for recommended alternative
- Draft In-Service Review (ISR) Checklist
- Interface documents
- Contractor SOW

8.3.3.3.5 Metrics

The metrics for this review consist primarily of the following:

- Customer Acclimation
- Number of system requirements that surface at later reviews compared to the original number of requirements
- Errata

If prototyping has been done to assist in finalizing the system requirements, then it would be possible to measure changes in the status of the TPPs. Otherwise, Technical Performance Measurement (TPM) would not be part of the metrics for this review.

8.3.3.3.6 Tools

The primary tools used for this review are:

- Requirements Database
- Risk Database
- Action Item Database
- Issues Database
- TPM Database (if used as a metric)
- SRR Risk Reduction Checklist

8.3.3.4 Preliminary Design Review (PDR)

The PDR is a formal review that assesses the preliminary design against the Allocated baseline and confirms that the preliminary design logically follows the SRR findings and meets the requirements. It normally results in approval to begin detailed design. Many organizations see it as the last viable point for effective technology insertion.

The preliminary design describes the system functions allocated to the subsystem and configuration item level. The solution design definition lacks considerable detail and is represented by the functional, performance, and interface requirements included in the Type B and Type C Specifications, and the draft Interface Control Documents (ICD). The PDR demonstrates that the preliminary design meets system and program requirements as specified in the Type A Specification previously approved. As part of the process of determining whether the design meets requirements, values for all TPPs allocated to the design are projected and compared with the target values and critical limits set during investment analysis. The results of the TPM analysis become part of the output of the PDR. Additional TPPs might be added depending on design or requirement changes approved at the PDR. Critical performance limits might also be adjusted based on approved requirement changes.

8.3.3.4.1 Timing and Relationship to AMS

The PDR is conducted at completion of functional allocation activities by the contractor and prior to the beginning of detailed design. (See Figure 36, FAA Product Development Process.)

8.3.3.4.2 Entrance Criteria and Inputs

The completed Allocated baseline as documented in design specifications for each hardware and software configuration item is the basis for conducting the review. Products previously completed by the contractor or provided as part of the contract that are required before proceeding to PDR include:

- List of allocated TPPs and associated critical performance limits and target values
- Constraints
- Type A Specification
- Functional Architecture
- IRDs
- Risk identification and mitigation plans
- Any proposed changes to the above items as a result of the work leading up to the PDR

Products that are to be submitted for review as part of the PDR include:

- Type B Specification (draft)
- Type C Specification, if needed (draft)
- Requirements Allocation Matrix (draft)
- ICDs (draft)

- Report on the results of the TPM analyses
- Preliminary design documentation (conceptual layouts, etc.)

8.3.3.4.3 Tasks

The following tasks are required to successfully accomplish the PDR:

- Define PDR objectives and scope
  - Establish success criteria and prerequisites (entry criteria, and approach to be used)
  - Set the date for the PDR and activities leading up to the review
  - Create an agenda for the review
  - Identify and notify participants and stakeholders of their roles and responsibilities.
- Identify the item(s) to be reviewed and the extent of review of each
- Compile the PDR-related data package. This package contains the PDR presentation material and all of the pertinent backup material.
- Distribute the PDR documentation to the stakeholder representatives and request timely review responses
- Obtain readiness approval for PDR and comments to the data package made via Review Item Discrepancy submissions
- Incorporate changes in the data package as needed
- Develop a summary of all concerns submitted and their respective answers
- Update risk mitigation plans based on review
- Conduct PDR with the incorporated changes
- Document and publish PDR minutes
- Compile action item and issues lists
- Track action items and issues
- Document closed action items and distribute to the PDR stakeholders

8.3.3.4.4 Exit Criteria and Outputs

Successful completion of PDR results in the approval to begin detail design and includes the following outputs:

- Updated Risk Mitigation plans to include risks identified during PDR
- RFA(s) with approved action plans
- Approved allocated baseline
  - Preliminary Type B Specification
  - Preliminary Type C Specification
  - Requirements Allocation Matrix
  - Preliminary ICDs
- Approved changes to the Type A Specification
- Approved changes to the functional architecture
- Approved changes to the IRDs
- Approved TPM report and approved changes to the TPPs
- Resolution of any contract scope issues revealed during the PDR process

8.3.3.4.5 Metrics

The PDR metrics are:

- Customer Acclimation
- The number of new subsystem requirements that surfaces at later reviews or testing compared to the initial number of requirements
- The number of design features that changes, compared to the original number, as a result of inadequate analysis prior to the PDR
- The number of RFAs accepted with formal action plans

The status of the TPPs is also used as a metric to measure the progress of the program.

8.3.3.4.6 Tools

The primary tools used for this review are:

- PDR Risk Reduction Checklist (see file TBD)
- Requirements Database
- Risk Database
- Action Item and Issues Database
- TPM Database

8.3.3.5 Critical Design Review (CDR)

The CDR is a formal review conducted to evaluate the completeness of the design, its interfaces, and suitability to start initial manufacturing. The CDR evaluates the design of a system or Configuration Item (CI) down to the lowest design level. It assesses the preliminary system product design package against the Allocated baseline and is conducted during the design and development phase of a program when detail design is essentially complete. The review:

- Determines that the detail design of the system or CI under review satisfies the performance and engineering specialty requirements of the Preliminary Hardware Product Specifications or Hardware Configuration Item (HWCI) development specifications. This includes projecting values for all TPPs allocated to the design and comparing them to the target values and critical limits previously set. The results of the TPM analysis become part of the CDR output.
- Establishes the detail design compatibility between the configuration items and other items of equipment, facilities, computer software, and personnel.
- Assesses system or CI risk areas (on a technical, cost, and schedule basis).
- Assesses the results of the producibility analyses conducted on system hardware.
- Reviews the preliminary hardware and/or software product specifications. For Computer Software Configuration Items (CSCI), this review focuses on determining the acceptability of the detailed design, performance, and test characteristics of the design solution and on the adequacy of the operation and support documents.

8.3.3.5.1 Timing and Relationship to AMS

Figure 36: FAA Product Development Process shows the CDR occurring during Solution Implementation at completion of CI detail design activities and prior to fabrication of hardware and/or coding of final software modules (typically the "90 percent" design point).

C3.5.2 Entrance Criteria and Inputs

Products previously completed by the contractor or provided as part of the contract that are required before proceeding to CDR include:

- Allocated Baseline (i.e., Type A Specification, IRDs, functional architecture, etc.)

- List of allocated TPPs and associated critical performance limits and target values
- Constraints
- CDR Planning documentation
- Master Verification Plan
- Risk identification and mitigation plans
- Previous review(s) RFAs and action items
- Any proposed changes to the above items as a result of the work leading up to the CDR

Products that are to be submitted for review as part of the CDR include:

- Detailed Type B and Type C Specifications
- Detailed Requirements Allocation Matrix
- Detailed ICDs
- Subsystem Functional Architecture
- Completed design package for each hardware and software CI (assembly layouts, etc.) with supporting design documentation
- Draft test plans
- Report on results of the TPM analyses
- Requirements Compliance Matrix for each CI

8.3.3.5.2 Tasks

The following tasks are required to accomplish a successful CDR:

- Define CDR objectives and scope
  - Establish success criteria and prerequisites (entry criteria and approach to be used)
  - Set the date for the CDR and activities leading up to the review
  - Create an agenda for the review
  - Identify and notify participants and stakeholders of their roles and responsibilities
  - Identify the item(s) to be reviewed and the extent of review of each
- Compile the CDR-related data package. This package contains the CDR presentation material and all of the pertinent backup material.
- Distribute the CDR documentation to the stakeholders and request timely review responses
- Obtain readiness approval for CDR and comments to the data package made via Review Item Discrepancy submissions
- Incorporate changes in the data package as needed
- Develop a summary of all concerns submitted and their respective answers
- Update risk mitigation plans based on review
- Conduct CDR with the incorporated changes
- Document results of CDR and publish CDR minutes
- Compile action-item list
- Track approved action items
- Document closed action items and distribute to the CDR stakeholders

8.3.3.5.3 Exit Criteria and Outputs

Successful completion of the CDR results in customer concurrence that the detailed design satisfies the system functional and performance requirements and is ready to begin fabrication. The CDR outputs or exit criteria are:

- RFA(s) with approved action plans
- Approved changes to Allocated baseline elements
- Approved TPM report
- Updated Risk Mitigation Plans to include risks identified during CDR
- Resolution of any contract scope issues revealed during the CDR process

8.3.3.5.4 Metrics

The CDR metrics are:

- Customer (Stakeholder) Acclimation, which is defined as the extent of satisfaction in the results of the CDR meeting the stated objectives. This can be measured through interviews and/or feedback forms for each presentation made during each review (incremental as well as final).
- The percentage of CDR-required data available on schedule. In the case of a technical review involving a supplier, this can be measured as the percent of review-related CDRLs submitted on schedule.
- The number of new subsystem requirements that surfaces at later reviews or testing compared with the initial number of requirements. A variation is to measure the number of scope issues that result in some contractual action.
- The number of RFAs accepted with formal action plans

The status of the TPPs is also used as a metric to measure the progress of the program.

8.3.3.5.5 Tools

The primary tools used for this review are:

- CDR Risk Reduction Checklist
- Requirements Database
- Risk Database
- Action Item and Issues Database
- TPM Database

8.3.3.6 Verification Readiness Review (VRR)

The Verification Readiness Review is a formal review of the contractors' readiness to begin product technical evaluation (i.e., verification including testing) on both hardware and software configuration items.

8.3.3.6.1 Timing and Relationship to AMS

The VRR is conducted at completion of system fabrication and prior to initiation of formal verification activities (see Figure 36: FAA Product Development Process).

8.3.3.6.2 Entrance Criteria and Inputs

These include the following:

- System definition is under formal configuration control
- All verification plans are approved.
- Draft verification procedures are available.

- Verification assets/resources are identified and available.

8.3.3.6.3 Tasks

Please refer to Section **Error! Reference source not found.**: **Error! Reference source not und.** for task details.

8.3.3.6.4 Exit Criteria and Outputs

Successful completion of the VRR results in approval to begin formal verification. The outputs include the following:

- Updated Risk Mitigation Plans to include risks identified during VRR
- Detailed verification procedures

8.3.3.6.5 Metrics

(Reserved)

8.3.3.6.6 Tools

VRR Risk Reduction Checklist

8.3.3.7 Functional Configuration Audit (FCA)

FCA is a formal review to verify that the as-built system and all subsystems can perform all their required design functions in accordance with their functional and allocated configuration baselines. (Figure 73 below describes the FCA process.) FCA supports completion of the PCA.

The FCA documents stakeholder approval of verification that a CI's actual performance fulfills the functional and performance requirements established in the system functional baseline. An FCA is held for each new configuration item or group of related configuration items. An FCA can also be held during the In-Service phase of a system's lifecycle to verify modifications and upgrades to a CI, or product and process improvements. The entry and exit criteria for this audit are to be included in the SEMP. An FCA is an incremental part of the system verification process. System changes that involve multiple CIs may require multiple audits. A final audit, or system verification review, is held to verify that all planned audits for a particular development have been successfully completed. Since the FCA relies on testing to determine if the CI meets all specified requirements, such testing is a prerequisite for the FCA. Figure 73 contains the process-based management chart for FCA.

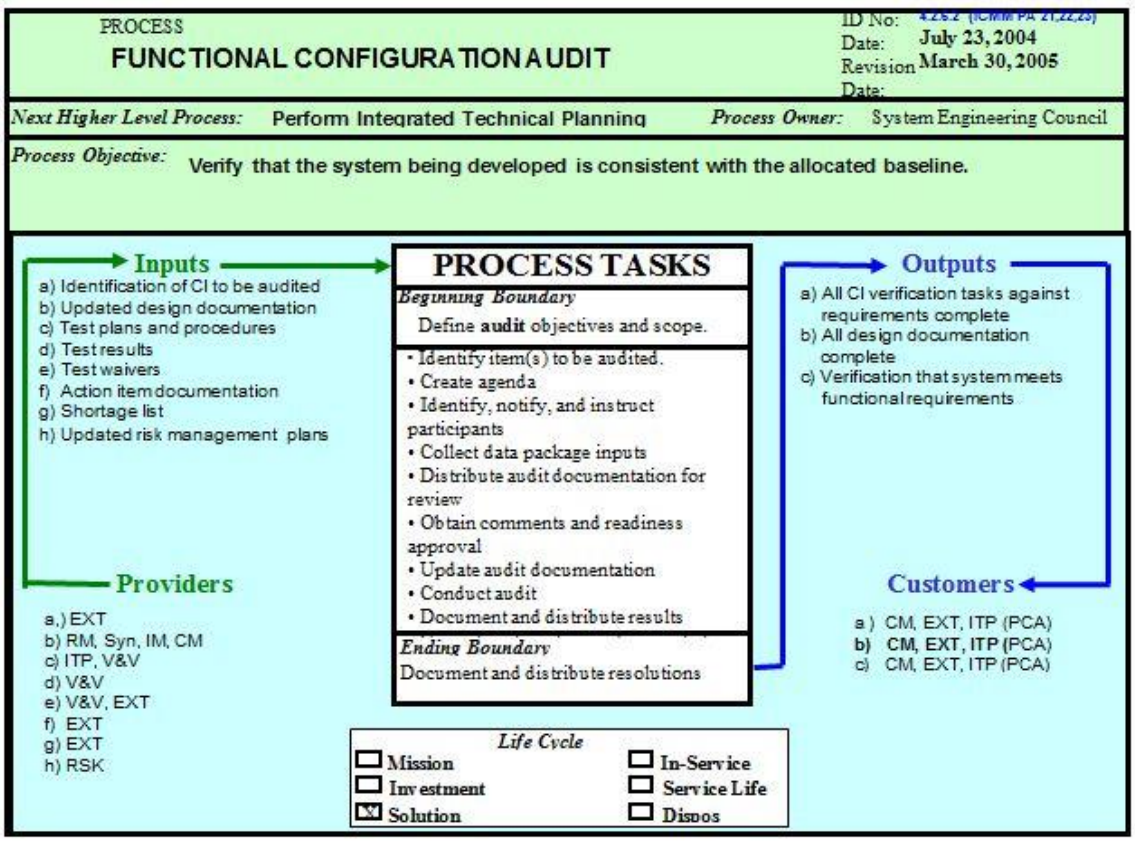


Figure 73: Functional Configuration Audit Process

8.3.3.7.1 Timing and Relationship to AMS

The FCA is conducted at completion of qualification and integration testing and prior to delivery of first production article.

8.3.3.7.2 Entrance Criteria and Inputs

These include the following:

- Verification program is complete.
- Verification reports are approved.
- Verification article configuration compliance to design package is established.

Basic inputs to the FCA include:

- Identification of the CI to be audited
- Update of all specification and design documentation complete (Specification Types A, B, and C; Requirements Allocation Matrix; ICDs; System Concept of Operations (ConOps); Subsystem Functional Architecture; Physical Architecture; and CI Description)
- All manufacturing process requirements and documentation finalized (Specification Types D and E)
- Test plans and procedures
- Test results
- A list of all deviations/waivers against the CI, either requested or customer approved
- A list of all action items for corrective action resulting from the test results
- Documentation of proposed corrective actions

- Complete shortage list
- Updated risk mitigation plans based on the test results

8.3.3.7.3 Tasks

The following tasks are required to successfully accomplish an FCA:

- Define FCA objectives and scope
  - Establish success criteria and prerequisites (entry criteria, and approach to be used)
  - Set the date for the FCA and activities leading up to the audit
  - Create an agenda for the audit
  - Identify, notify, and instruct participants and stakeholders concerning their roles and responsibilities
  - Identify the CI(s) to be audited and the extent of review of each
- Collect data package inputs for FCA briefing and documentation
- Distribute FCA documentation to stakeholder representatives for review for completeness, correctness, clarity, and organization
- Obtain readiness approval for FCA and comments to the data package made via audit worksheets
- Update FCA documentation per the worksheets
- Conduct FCA
  - Report on verification status — requirements verified versus planned corrective actions
  - Report on completeness of all development and design documentation, including planned revisions associated with corrective actions
  - Report on key issues identified in the review of the FCA documentation
  - Report on risk assessments and mitigation plans
  - Assign responsibility for corrective actions and documentation revisions
  - Obtain stakeholder approval to proceed
- Document and distribute the results of the FCA
- Compile action-item and issues list
- Track action items and issues
- Document and distribute the resolutions of action items and issues

8.3.3.7.4 Exit Criteria and Outputs

The key outcome of the FCA is to determine if there is any gap of required versus verified performance. The key FCA outputs are:

- Verification that the system meets functional requirements
  - Type A Specification verified
- Completion of all CI verification tasks against requirements
  - Type B Specification verified
  - Type C Specification verified
  - Requirements Allocation Matrix verified
  - ICDs verified

  - (Any) Gap of required versus verified performance documented
- Completion of all development and design documentation
  - Type A, B, and C Specifications
  - Requirements Allocation Matrix
  - ICDs
  - System Level ConOps
  - OSED
  - Functional architecture
  - Physical architecture
  - CI Description, including a Configuration reconciliation list between the articles in the verification program and the configuration defined by the design package

8.3.3.7.5 Metrics

The metric is customer approval of FCA and the number of open worksheets generated if the approval is conditional.

8.3.3.7.6 Tools

The primary tools for this audit:

- FCA Risk Reduction Checklist
- Requirements Database
- Action Item Database
- Issues Database

8.3.3.8 Physical Configuration Audit (PCA)

The PCA is a formal audit that establishes the Product Baseline for formal configuration control of the CI for Production and later Lifecycle phases. It assesses the as-delivered system's compliance with the product design and manufacturing documentation. Successful completion of the PCA marks the complete transfer of formal configuration control from the developer to the product owner.

> ***Tip:*** *The PCA is typically performed on an early production configuration item. The actual effectivity established for the PCA centers around the transfer of risk. Because formal configuration control occurs at this point, the issue of liability for changes becomes the issue. It is in the interest of the system owner to hold the audit as late as possible; the developer is looking to transfer the risk of changes to the owner as early as possible. Setting the actual effectivity often becomes a contractual or scope issue.*

The PCA documents the agreement of the stakeholders that the CIs actual configuration as built by the specified manufacturing processes conforms to the Technical Data Package that describes the CI baseline. The audit also ensures that the proper processes and procedures are in place to confirm the following:

- The CI design definition and planning are current.
- Hardware/software conforms to the design package and requirements, and that differences have been reconciled.
- Nonconformities have been reconciled in accordance with applicable procedures.
- The manufacturer has accomplished specified production tests.
- Part numbers and nomenclature of the CI are consistent with drawings and parts lists, and item nomenclature agrees with the approved nomenclature.

- Any configuration differences between the PCA unit and formal verification units have been identified, documented, and properly authorized for incorporation.
- The initial product baseline includes all authorized changes, current complete design and production packages, ICDs, and Acceptance Test procedures.

A PCA is held for each new configuration item or group of related configuration items. A PCA can also be held during the in-service phase of a system's lifecycle to verify modifications and upgrades to a CI or product and process improvements. The entry and exit criteria for this audit and any other pertinent accomplishment and associated success criteria are to be included in the SEMP. System changes that involve multiple configuration items may require multiple audits. A final audit is held to verify that all planned audits for a particular development have been successfully completed.

8.3.3.8.1 Timing and Relationship to AMS

The PCA is conducted after delivery of initial production unit and prior to Contractor Acceptance and inspection.

8.3.3.8.2 Entrance Criteria and Inputs

To conduct a successful PCA, two other control functions must have occurred: completion of the Independent Operational Test and Evaluation (IOT&E) and completion of the FCA.

Basic inputs to the PCA include:

- Identification of the CI to be audited
- Completion of the technical data package
  - Update of all specification and design documentation complete (Specification Types A, B, and C; Requirements Allocation Matrix; ICDs; System ConOps; Subsystem Functional Architecture; Physical Architecture; and CI Description)
  - Incorporate all required changes identified through the IOT&E
- Manufacturing and quality control plans complete and quality control results available
  - Update of all manufacturing process requirements and documentation completed (including Specification Types D and E)
- Configuration differences between FCA and PCA units reconciled
  - A list of all deviations/waivers against the CI, either requested or customer approved
- Complete shortage list
- Updated risk mitigation plans based on the FCA results

8.3.3.8.3 Tasks

The process-based management chart for the PCA (Figure 74) addresses the following tasks:

- Define the objectives and scope of the PCA
  - Establish success criteria and prerequisites (entry criteria, and approach to be used)
  - Set the date(s) for the PCA and activities leading up to the audit
  - Create an agenda for the audit
  - Identify and notify participants and stakeholders of their roles and responsibilities
  - Identify the CI(s) to be audited and the extent of review of each
- Review status of action items from the FCA to determine if they have been adequately resolved; identify any corrective action required

- Verify that all changes identified through the IOT&E have been incorporated; identify any corrective action required. Reconcile all proposed and actual configuration differences with the approved Product Baseline
- Conduct physical review of the CI and compare the configuration to the proposed baseline documentation; identify any corrective action required

Audits are typically performed at the facilities where the items or their selected subassemblies are produced. The producer shall ensure that suitable facilities and support are available. The PCA Plan should specify the items to be audited and their respective schedules.

> ***Tip**: The most common approach is to conduct a product audit where the selected item(s) is physically compared with its documentation. This approach is usually accomplished incrementally for complex systems by conducting individual audits on selected subassemblies and components leading to a final review at the system level. The items audited should be designated by serial number before their induction into the manufacturing process to minimize the amount of potentially destructive teardown or disassembly.*

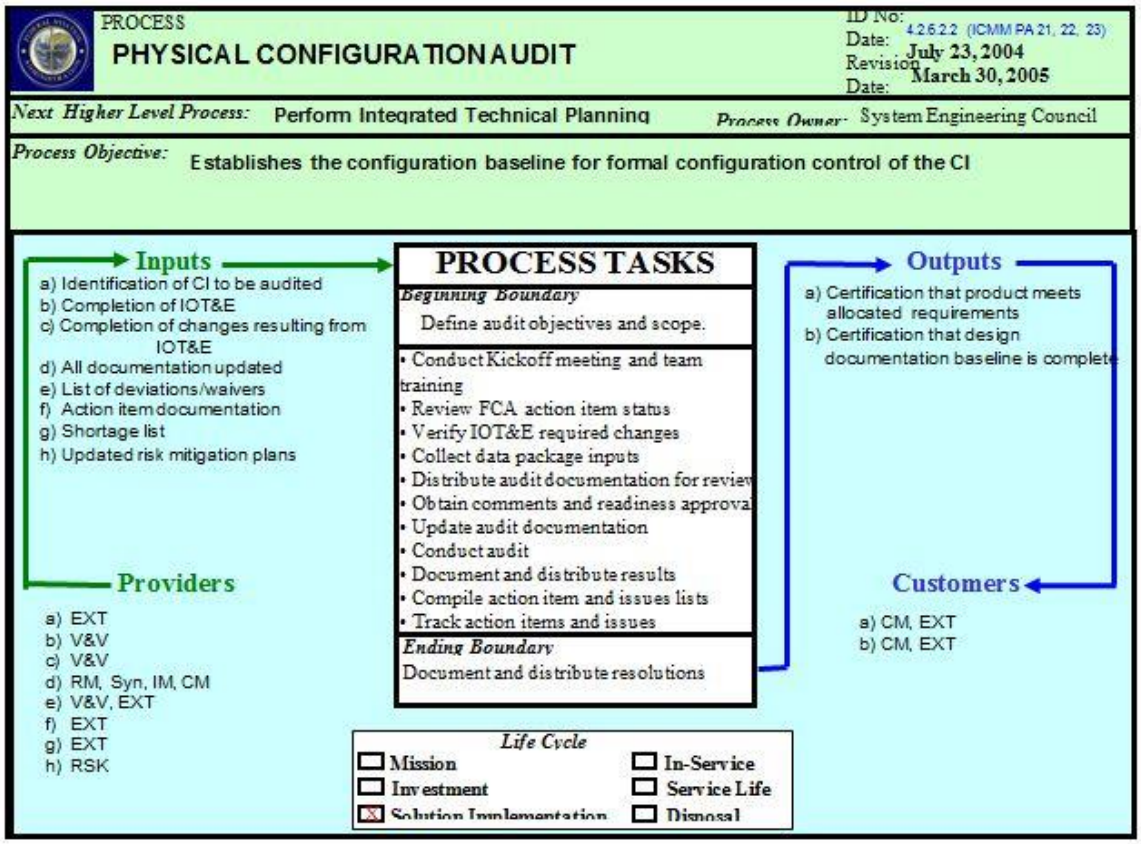


Figure 74: Physical Configuration Audit Process

> ***Tip:** For organizations that are ISO compliant, a process audit approach can be considered. The approach builds on the ISO process of periodic compliance sampling by identifying and determining if key processes are in place and compliant with the organization's ISO certification. To confirm the integrity of this approach, it is recommended that a single item be selected, and a one-time verification of its major processes be accomplished. To be successful, this verification must conclude that the item physically conforms to its design documentation and that all of its documentation in the process flow is adequate to support production and configuration control of that item.*

The process audit approach includes the following tasks:

- Collect data package inputs for PCA briefing and documentation
- Distribute PCA documentation to stakeholder representatives for review for completeness, correctness, clarity, and organization
- Obtain readiness approval for the PCA and comments to the data package made via PCA worksheets
- Update PCA documentation per the worksheets
- Conduct the PCA
    - Report on change status — changes incorporated versus planned corrective actions
    - Report on completeness of all development and design documentation, including planned revisions associated with corrective actions
    - Report on verification of consistency between CI and documentation, including planned corrective actions
    - Report on key issues identified in the review of the PCA documentation
    - Report on risk assessments and mitigation plans
    - Assign responsibility for corrective actions and documentation revisions
    - Obtain stakeholder approval to proceed
- Document and distribute the results of the PCA
- Compile action item and issues lists
- Track action items and issues via PCA worksheets
- Document and distribute the resolutions of action items and issues

8.3.3.8.4 Exit Criteria and Outputs

The result of a successful PCA is the issuance of a signed PCA Certificate. This signifies that the system has demonstrated compliance with its design package and that formal configuration control is ready to be transferred from the implementer to the owner of the item or system. The PCA is complete when the Certificate is “unconditional”; that is, issued without any open action items or non-compliances. If there are open action items or non-compliances (documented, tracked, and resolved via PCA worksheets), these are annotated on the PCA Certificate, and the certification is considered “Conditional.” Its status is changed to “unconditional” after all worksheet action plans are completed and accepted by the certifying party. The key outputs of the PCA are the following:

- Certification that product meets allocated requirements
    - Types A, B, and C Specifications verified
    - Requirements Allocation Matrix verified
    - ICDs verified
- Completion of all development and design documentation
    - Type A, B, and C Specifications
    - Requirements Allocation Matrix
    - ICDs
    - System Level ConOps
    - OSED
    - Functional architecture

- Physical architecture
- CI Description
- User manuals

8.3.3.8.5 Metrics

The primary metric is the Customer's issuance of a PCA Certificate signifying unconditional completion of this milestone. Interim metrics include the number of worksheets generated/open (conditional completion) and/or the number of incremental PCAs completed (if an incremental approach is used).

8.3.3.8.6 Tools

The primary tools used for this audit are:

PCA Risk Reduction Checklist (see file TBD)

- Requirements Database
- Action Item Database
- Issues Database

8.3.3.9 In-Service Performance Review (ISPR)

The ISPR is a formal technical review to characterize In-Service technical and operational health of the deployed system by providing an assessment of risk, readiness, technical status, and trends in a measurable form that will substantiate In-Service support and budget priorities. It is intended to evaluate performance against baseline values and customer expectations. Post-implementation review(s) at deployment sites help to determine whether performance and benefits in the Exhibit 300 Program Baseline are being achieved. When projections are not being realized, corrective action is planned and implemented. Periodic operational evaluations of fielded assets continue throughout In-Service Management to identify performance shortfalls, determine trends in the cost of ownership, and identify adverse support trends. These evaluations are the basis for revalidating the merit of sustaining investment assets or the need for other action. Findings are fed back into service analysis, where it is determined whether to continue to sustain existing assets or recommend new investments to solve systemic operational problems in the service environment.

8.3.3.9.1 Timing and Relationship to AMS

The In-Service Management phase begins when the new system, software, facility, or service goes into operational use and continues for as long as the product is in use. This phase is characterized by a continuing partnership among the providing, operating, and support organizations. This review is typically held a minimum of two years after introduction of the new capability into the operational NAS environment.

8.3.3.9.2 Entrance Criteria and Inputs

(Reserved)

8.3.3.9.3 Tasks

(Reserved)

8.3.3.9.4 Exit Criteria and Outputs

The outcome of this review is a decision on whether a configuration item (or system) has reached the end of its useful life or is no longer satisfying an identified need. The outcome may span a range of recommendations—from a strategy of continued support of the installed capability to a decision to obsolete the existing system and enter the Mission Analysis phase to address the resulting predicted need shortfall. (See Section 5.2: Life Cycle Engineering, for further discussion of this outcome.)

8.3.3.9.5 Metrics

(Reserved)

8.3.3.9.6 Tools

The primary tools used for this audit are:

- The PCA Risk Reduction Checklist

8.3.4 FAA System Engineering Inputs to Related Reviews

Each SE control gate or milestone fits within the AMS framework and supports various investment decisions. The entry and exit criteria for both the SE milestones and AMS investment decision points are addressed to provide the reader visibility into the extent of overlap between the two needs.

8.3.5 Investment Analysis Readiness Review (IARR)

(Reserved)

8.3.5.1 Integrated Baseline Review (IBR)

(Reserved)

8.3.5.2 In-Service Review (ISR)

(Reserved)

8.3.6 Request for Action (RFA) Forms and Process

(Reserved)

8.4 Appendix D: Example of Using PDCA

The PDCA (Plan, Do, Check, Act) cycle can be applied to many things. The following Safety Improvement or eliminating accidents example shows PDCA in action.

Plan

Identify the problem. You notice an increase in lost time and medical claims due to accidents over the past year. The organization has installed some new equipment and hired a significant number of new employees who replaced retiring personnel. In some areas new energy-efficient lighting has been installed. The lost time and medical claims are costing the organization a lot of money.

Analyze the problem. What is the cause of the accidents? Who is getting injured? Did the change in lighting contribute to the accidents? Are the new employees properly trained? Are the new employees more distracted than more senior workers? Are new procedures needed for the new equipment?

Your analysis shows that primarily new employees are the ones getting injured. An approved lighting analysis method shows that task lighting is still adequate. There has been some on-the-job training for the new employees, but many of the senior workers have retired. The organization needs to resolve the safety issues to remain profitable.

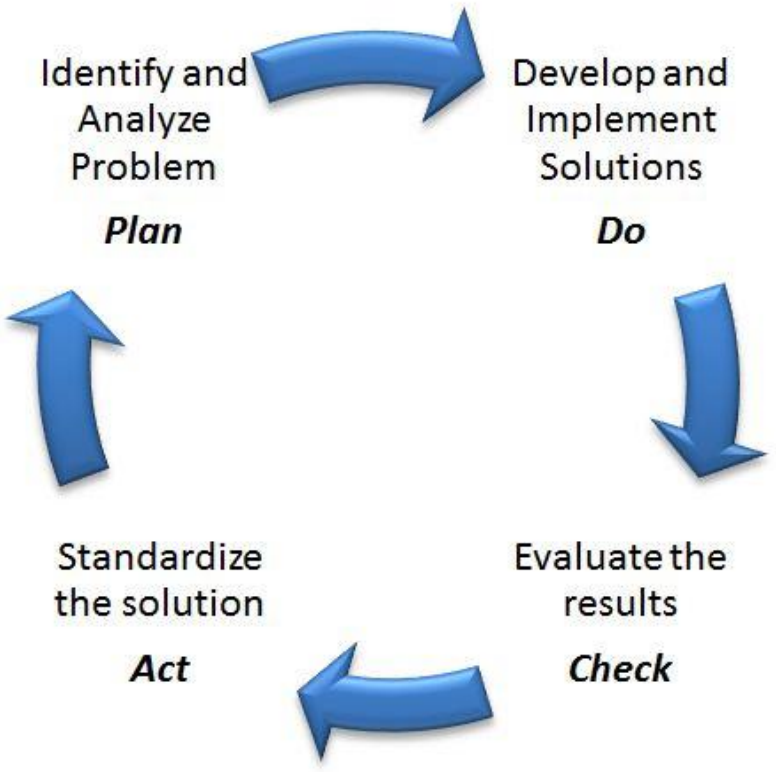


Figure 75: PDCA Cycle – Safety Improvement Example

Do

Develop solutions. You could ensure that the organization's procedures are still appropriate for the new equipment. You could develop a formal training course for the newer employees. Should you use an outside organization to conduct the training?

Implement the solution. You decide to hire some retired former employees to conduct training for the newer employees.

Check

Evaluate the results. Conducting training for the new employees reduced the number of lost days and injury claims.

Was the desired goal achieved? If so, go to the act step. If not, go to the plan step.

If you go to the plan step you could plan a review on the organizational procedures for using the machines. Do the new machines operate the same as the ones they replaced? (Note: If this is done, this would be the second iteration of Plan and Do.}

Act

Standardize the solution. If the problem ever occurs again, you will be prepared to conduct training for the new employees. To prevent future occurrences, you establish a training program for all new employees.

The following references might be useful to those seeking more information on PDCA.

References and Useful Information	**Useful for Section**
Shewhart, Walter Andrew (1939). *Statistical Method from the Viewpoint of Quality Control*. New York: Dover. ISBN 0-486-65232-7.	1.4
Deming, W. Edwards (1986). *Out of the Crisis*. MIT Center for Advanced Engineering Study. ISBN 0-911379-01-0.	1.4
Anderson, Chris. How Are PDCA Cycles Used, *Bizmanualz*, June 7, 2011.	1.4
http://en.wikipedia.org/wiki/File:PDCA_Cycle.svg?qsrc=3044	1.4
ISO 9001 Quality Management Systems - Requirements. ISO. 2008. pp. vi.	1.4