

## 4.1 PERFORM SYSTEM ENGINEERING

### 4.1.1 Introduction to System Engineering

The Federal Aviation Administration (FAA) System Engineering (SE) method is robust, iterative, and has extensive interdependencies among the SE elements listed in Table 1.2-1 in Chapter 1. The process workflow (see Figure 4.1-1) captures the essence of these linkages and provides a high-level view of the various SE processes and how they functionally interact. These functional interfaces only represent the predominant interaction between each process. The interaction between processes at a lower level is much more involved (i.e., Figure 4.1-1 is a simplified view and does not depict all the ways that processes interact). Figure 3.1-2 (Chapter 3) is an N-squared ( $N^2$ ) diagram of SE that shows the actual work products exchanged between the various SE processes shown in Figure 4.1-1.

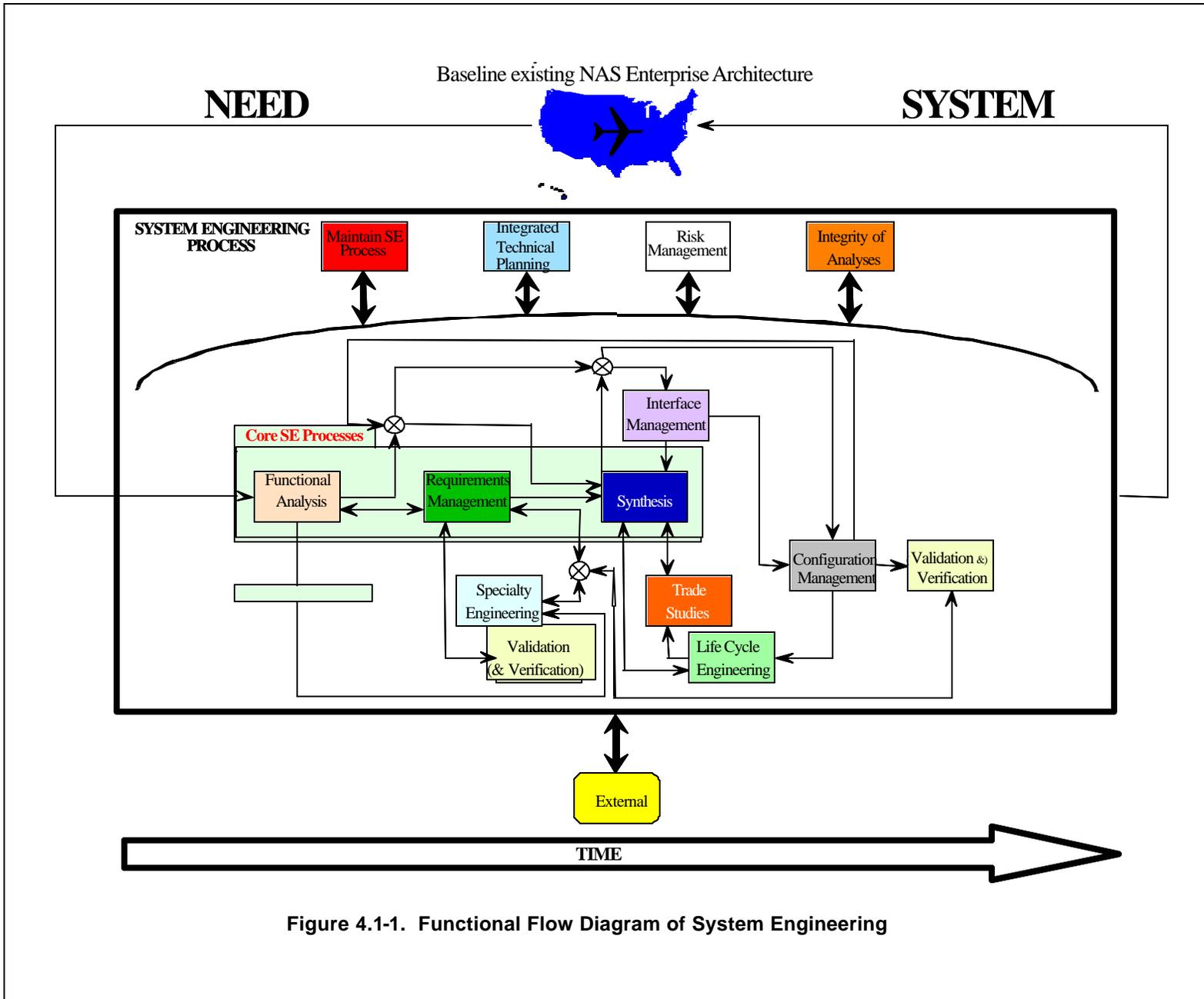


Figure 4.1-1. Functional Flow Diagram of System Engineering

In Figure 4.1-1, each SE process is laid out from left to right to notionally depict when in time each process is employed relative to another. The time arrow is **not** relative to the AMS lifecycle phases. Note that overall SE, and many of the interactions at the lower levels, may be iterative in nature; thus, the left-to-right timeline is notional.

Figure 4.1-1 indicates that SE is initiated when there is a need; that is, a recognized shortfall in capability within the NAS. One of the tools or products used to determine need or identify a shortfall in service capability is the National Airspace System (NAS) Enterprise Architecture (EA). The EA defines the mission, the information necessary to perform the mission, and the technologies necessary to perform the mission. It is used to manage change when implementing new technologies in response to changing mission needs. The EA includes a baseline architecture (or existing NAS), target architecture(s), and a transition plan. It is divided into a number of views or perspectives on the information in the architecture. As presently defined, the FAA EA builds on the approach that the U.S. Department of Defense (DoD) uses to define its EA, the DoD Architecture Framework (DoDAF). There are three types of views in the DoDAF: the all views (AV), the operational views (OV), and the system view (SV). The AV states the purpose of the architecture and provides an integrated dictionary. The OV provides the specification of tasks, operation elements, and information exchanges required to accomplish the mission. The OV also defines the types of information exchanges, the frequency of exchange, which activities are supported by the information exchanges, and the maturity of the information exchanges. The SV describes the system(s) and interconnections providing for or supporting FAA functions and associated systems resources to the operational activities to facilitate the exchange of information among operational nodes (e.g., facilities). Each subsequent Chapter 4 section (Sections 4.2 through 4.14) will describe the EA product(s) that directly or indirectly relate to that particular SE process element and products.

Stakeholder needs may arise as a result of a new service to be provided or with the advent of technological innovations to be leveraged to reap improvements in capacity, efficiency, security, and/or safety. Once the need is validated, the Functional Analysis process (Section 4.4) is performed to develop Concepts (see Figure 4.1-1). The Requirements Management process (Section 4.3) uses the Concept of Operations to develop a Service Level Mission Need, which is then fed back to Functional Analysis as input to develop the highest level of functional architecture for the new or modified system. The Requirements Management process uses this high-level functional architecture, as well as inputs from Specialty Engineering analyses, to develop requirements. The Validation and Verification process (Section 4.12) validates these requirements. Interaction between Functional Analysis and Requirements Management is iterative, as the functional architecture and resulting requirements are decomposed to a level necessary to the appropriate requirements that describe the needed system characteristics. Synthesis (Section 4.5) then develops the physical architecture or design solution to those requirements.

Along with these initial SE activities, three overarching processes that interact with all SE processes are employed. These processes, which continue throughout the system's lifecycle, are as follows:

- Integrated Technical Planning (Section 4.2)
  - Provides the technical guidance tools required to track and manage program activity
- Risk Management (Section 4.10)

- Provides an organized, systematic decision-making approach to identify risks that affect achievement of program goals
- Analyzes identified risks
- Mitigates risks effectively
- Tracks the progress of the mitigation efforts
- Integrity of Analyses (Section 4.9)
  - Ensures provision of credible, useful, and sufficient data/results for program management's decision-making process
  - Ensures the integrity and fidelity of the various analysis tools

Once a valid set of requirements is obtained, the Synthesis process (Section 4.5) is initiated to define system elements and to refine and integrate these elements into a physical architecture. In addition to the requirements input into the Synthesis process, the functional architecture is provided to clarify and bound the system. The Trade Studies process (Section 4.6) and the Lifecycle Engineering process (Section 4.13) supply cost estimates to support the Synthesis process, which ultimately determines the design alternative that best satisfies the identified stakeholder need.

Interface Management (Section 4.7) plays a key role in ensuring that the various internal system pieces are coordinated as well as integrated with external systems. As the total system is decomposed via iterative interaction of Functional Analysis, Requirements Management, and Synthesis, physical and functional interfaces are identified and managed.

The results of these SE activities are continually placed under Configuration Management (Section 4.11). The system is developed according to the baseline design and verified with the Validation and Verification process (Section 4.12). With the system verified as able to meet the identified stakeholder need, it is deployed into the NAS. Although the discussion of this simplified view and description of SE was sequential, SE is truly iterative and employed continuously throughout the lifecycle of the system.

When used properly, SE creates an infrastructure that ensures that customer requirements and expectations are effectively and efficiently identified, integrated, and managed. Because the primary objective of SE is to provide a balanced view of needs and solutions, the integration dimension of this effort should not be underestimated. **Integration is defined as the progressive linking and testing of system components to merge their functional and technical characteristics into a comprehensive, interoperable system.**<sup>1</sup> From a process perspective, it can be viewed as the conduits connecting the elements, as well as the overall SE framework to its environment, in Figure 4.1-1. From a system perspective, it can be viewed as the glue that binds the various elements of a product, transforming it from a confederation of loosely related items to a tightly coupled entity.

Each SE element is capable of maximizing the thoroughness and quality of interaction and cooperation between individuals, teams, suppliers, and stakeholders as each SE element is performed. In addition, each SE element plays various roles throughout the lifecycle phases as shown in Table 3.2-1 (Chapter 3). The following subsections provide an overview of each SE

---

<sup>1</sup> Institute for Telecommunications, U.S. Dept of Commerce.

element regarding its objective, definition, and value. The subsequent sections of the manual (Sections 4.2 through 4.14 and the appendices) extensively document each SE element and contain these details:

- Process-Based Management (PBM) chart (objectives, inputs, and associated providing process (providers); outputs and associated receiving process (customers); process tasks; and applicable lifecycle phases)
- Process workflow
- Methods, tools, and detailed descriptions of how the tasks of each SE element are accomplished
- Steps to tailor the SE element
- Appendices for terms, acronyms, and work product examples

#### 4.1.2 Summary of System Engineering Areas

The following subsections briefly summarize FAA SE and its 13 elements. The bracketed information under each subsection heading provides a cross-reference to the applicable section number and the relevant integrated Capability Maturity Model (iCMM) process areas. The iCMM uses process areas to describe the process attributes. Process areas group together base practices related to achieving goals and a common purpose. Table 4.1-1 lists the iCMM Process Areas.

**Table 4.1-1. iCMM Process Areas**

PA 00 Integrated Enterprise Management	PA 12 Supplier Agreement Management
PA 01 Needs	PA 13 Risk Management
PA 02 Requirements	PA 14 Integrated Teaming
PA 03 Design	PA 15 Quality Assurance and Management
PA 04 Alternatives Analysis	PA 16 Configuration Management
PA 05 Outsourcing	PA 17 Information Management
PA 06 Design Implementation	PA 18 Measurement and Analysis
PA 07 Integration	PA 19 (reserved for future use)
PA 08 Evaluation	PA 20 Process Definition
PA 09 Deployment, Transition, and Disposal	PA 21 Process Improvement
PA 10 Operation and Support	PA 22 Training
PA 11 Project Management	PA 23 Innovation

### 4.1.2.1 System Engineering

[SEM 4.1; iCMM PA 01 through 05, 07 through 14, 16, and 20 through 23]

#### 4.1.2.1.1 Objective

The objective of SE within the FAA is to consistently provide balanced solutions to complex FAA system needs.

#### 4.1.2.1.2 Definition

*SE is 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 aspect.*

SE defines how the organization discerns a problem, how it approaches developing a solution to a problem, and how it implements the plan to enable resolution of the problem.

#### 4.1.2.1.3 Value

While SE process elements support the cycle defined by the Acquisition Management System (AMS), they also provide a finer, more detailed breakdown that provides better management visibility into the operation of the program. This leads to earlier identification of issues, problem correction, and better identification of requirements, which reduces risk as well as cost. Support organizations are better able to gauge and plan their work to support each phase.

### 4.1.2.2 Integrated Technical Planning

[SEM 4.2; iCMM PA 11, 21, 22, 23]

#### 4.1.2.2.1 Objective

The Integrated Technical Planning element (Section 4.2) seeks to provide program management with specific guidance and direction on how to plan a program's execution resulting in a sound, repeatable method for performing a requirements-based and structurally managed program. It also provides a feedback mechanism (subsection 4.2.6) 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.

#### 4.1.2.2.2 Definition

Integrated Technical Planning 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 technical plans provide stakeholder- and contract-driven tailoring of SE to optimally satisfy program needs. These plans are living documents that are kept current throughout the program's lifecycle.

Technical reviews and audits are the primary means to monitor and control performance to the technical plans. They provide insight into the readiness of a program to proceed to each subsequent phase of the system's lifecycle.

#### **4.1.2.2.3 Value**

Various levels of technical and program management use the technical plans that result from Integrated Technical Planning. Expending upfront effort to generate clear, complete, and correct technical plans results in consistent performance across the program. A consistent focus on monitoring implementation progress reduces the risk of missing program objectives. Optimally, miscommunication and misinterpretation of stakeholder and executive expectations by individuals are eliminated. Developing and following properly prepared plans assist in eliminating miscommunication and helps the program to adapt to changes in program environment.

#### **4.1.2.3 Requirements Management**

[SEM 4.3; iCMM PA 01 and 02]

##### **4.1.2.3.1 Objective**

The Requirements Management element (Section 4.3) seeks to identify and develop all requirements and ensure that they are met throughout the product's lifecycle. It is an iterative process that:

- Identifies and captures the requirements applicable to the system
- Analyzes and decomposes the requirements into clear, unambiguous, traceable, and verifiable requirements
- Allocates the requirements to the appropriate component within the system hierarchy and/or to the appropriate organizational entities
- Derives lower level requirements from higher level requirements in the system hierarchy
- Establishes the method of verification for each requirement
- Ensures that the product complies with the requirements
- Manages, documents, and controls the requirements and changes to them in a traceable manner

##### **4.1.2.3.2 Definition**

Requirements Management is a process performed throughout a system's life to elicit, identify, develop, manage, and control requirements and associated documentation in a consistent, traceable, correlatable, and verifiable manner. Requirements Management iteratively identifies and refines the top-level requirements to successively lower levels in concert with functional baselines and architectures and synthesis of solutions established for the system of interest.

The Requirements Management element consists of a series of iterative tasks that a multifunction team performs throughout all AMS phases. The team's focus is to elicit, develop, manage, and control requirements and associated documentation. Once the team defines the requirements, it uses a disciplined Requirements Management methodology to manage the

requirements set, helping to ensure compliance with stakeholder needs and expectations, communication of allocations, and adaptation to/control of changes.

#### **4.1.2.3.3 Value**

Requirements fuel the design process. They define the characteristics of a system at all levels of complexity. They are derived from multiple inputs from internal and external sources that need to be logically and efficiently collected and synthesized in a centralized, accessible decision database. The information collected, managed, and controlled is accessed by various teams within the stakeholder and program organizations, associated internal interfaces (e.g., management or operations), and contractors/suppliers. When Requirements Management is performed well, rework and poorly communicated information typically is minimal, if not eliminated entirely. Furthermore, this process is used to reveal gaps, redundancies, biases, and/or inconsistencies and resolve, revise, and/or refine them in a consistent, integrated method that satisfies all the stakeholders. The solid foundation built through Requirements Management provides an ongoing resource for all program stages.

#### **4.1.2.4 Functional Analysis**

[SEM 4.4; iCMM PA 03 and 04]

##### **4.1.2.4.1 Objective**

The Functional Analysis element (Section 4.4) seeks to provide a framework for developing requirements and physical architectures that significantly improves innovation, synthesis of design, requirements development, and product integration.

##### **4.1.2.4.2 Definition**

Functional Analysis translates stakeholders' needs into a sequenced and traceable functional architecture. It pinpoints innovative design solutions and sheds light on vague interfaces. It also provides the basis for logical and realistic product integration and synthesis. As the analyses are performed, additional requirements often are flushed out/derived, thereby providing the program a more detailed list of requirements and an increased understanding of the system. The functional architecture defines what the system does, including interfaces (both within the system and to the external world).

##### **4.1.2.4.3 Value**

The Functional Analysis process provides two key benefits to SE: It discourages single-point solutions, and it describes the behaviors that lead to requirements and physical architectures. The functional architecture and functional interfaces enable the stakeholders and program management to logically develop requirements down to the lowest level of a system hierarchy.

##### **4.1.2.5 Synthesis**

[SEM 4.5; iCMM PA 03 and 04]

#### 4.1.2.5.1 Objective

The Synthesis element (Section 4.5) seeks to define design solutions and identify systems that will satisfy the program requirements. Synthesis translates the requirements, as set in context by the functional architecture, into the design architecture, consisting of the physical architecture with its associated technical requirements.

#### 4.1.2.5.2 Definition

Synthesis is the creative process that translates requirements (performance, function, and interface) into alternative solutions. This results in a physical architecture for the “best-value” design solution composed of people, products, and process solutions for the logical, functional grouping of the requirements.

The synthesized design generated is a balanced (i.e., cost, quality, schedule, risk, performance, producible/supportable) solution and is created through analysis of candidate elements. The candidate elements are preliminarily defined and then iteratively defined down to lower, more detailed levels until refinement of the system concept is complete.

#### 4.1.2.5.3 Value

A series of benchmarks for various design performance parameters (e.g., power, data storage, testability, and reliability) are generated and used to measure the viability and worth of a candidate design solution. Design performance parameters, ranked by importance, are refined during the design evolution of an affordable, responsive system design. Throughout the evolutionary analyses, credibility and acceptability by the stakeholders shall be ensured. The iterative nature of the candidate element task provides the mechanism to continuously correct design inadequacies and to refine the physical allocation process. The task also provides opportunities for new technologies and innovative ideas to be considered, justified, and integrated. These efforts are used to validate the synthesized design in terms of balance, completeness, understandability, and reflection of the stakeholders’ requirements.

#### 4.1.2.6 Trade Studies

[SEM 4.6; iCMM PA 04]

##### 4.1.2.6.1 Objective

The Trade Studies element (Section 4.6) seeks to select the most balanced (i.e., cost, schedule, quality, and risk) solutions from a set of proposed viable alternatives based on defined criteria.

##### 4.1.2.6.2 Definition

Multidisciplinary teams use the Trade Studies element to confirm that the most balanced technical solutions have been identified. The team methodically evaluates a series of design alternatives and recommends the preferred feasible solutions that enhance the value and performance of the overall system and/or functions. The team details each assessment to an appropriate level that allows differentiation between alternatives. The team develops recommendations and forwards them in a trade study report to the appropriate decision maker(s) (e.g., program management or stakeholders) for action.

#### 4.1.2.6.3 Value

Trade Studies element tasks are designed to assist decision makers. The thorough identification and assessment of multiple facets of a problem aid the decision maker to relate the whole problem to optimal, feasible solutions by comparing technical, cost, and schedule interactions. The Trade Studies element prevents program/project management from committing too early to a design that may not be cost effective or meet all system requirements too early in the process. It provides the traceability to substantiate design and configuration changes to the baseline product design; it also documents why one alternative was chosen over another during the decision-making process. The appropriate management authority uses this information to make a final decision.

#### 4.1.2.7 Interface Management

[SEM 4.7; iCMM PA 07]

##### 4.1.2.7.1 Objective

The Interface Management element (Section 4.7) seeks to identify, describe, and define interface requirements to ensure compatibility between interrelated systems and between system elements, as well as provide an authoritative means of controlling the interface design.

##### 4.1.2.7.2 Definition

Interface Management, which includes identifying, defining, and controlling interfaces, 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.

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 occur within the system (internal) as well as between the instant system and another system (external).

The Interface Requirements Document (IRD) records interface requirements. The Interface Control Document (ICD) contains the "as built" design of how the contractor implements the requirements.

##### 4.1.2.7.3 Value

During the program's life, compatibility and accessibility shall be maintained for the many diverse elements. Compatibility analysis of the interface definition demonstrates completeness of the interface and traceability records (or lack thereof). As changes are made, an authoritative means of controlling the design of interfaces shall be managed with appropriate documentation, thereby avoiding the situation in which hardware/software, when integrated into the system, fails to function as part of the system as intended. Ensuring that all system pieces work together is a complex task that involves teams, stakeholders, contractors, and program management, from the end of the initial concept definition stage through the operations and support stage.

#### 4.1.2.8 Specialty Engineering

[SEM 4.8; iCMM PA N/A]

#### 4.1.2.8.1 Objective

The Specialty Engineering element (Section 4.8) seeks to: (1) integrate specific system attributes and disciplines into the acquisition process; and (2) assess and confirm various system attributes (Specialty Engineering).

SE relies on specialty domain expertise to define and characterize specific requirements. SE's function in this process is to integrate the design engineer's activities and specialty engineer's activities; coordinate and open communication lines between the design engineer and specialty engineer; and focus the engineering effort on meeting the common goal of satisfying the customer.

#### 4.1.2.8.2 Definition

The Specialty Engineering element defines and evaluates a system's specific areas, features, or characteristics as related to the specialty engineering aspects of the system. Specialty Engineering analyses describe technical details of the design from a particular perspective and often require specialized skills. Table 4.1-2 describes, generally, the Specialty Engineering disciplines.

**Table 4.1-2. Specialty Engineering Disciplines**

<b>Specialty Engineering Discipline</b>	<b>Description</b>
System Safety Engineering (SSE)	Evaluation and management of the safety risk associated with a system using measures of safety risk identified in various hazard analyses, fault tree analyses, safety risk assessments, and hazard tracking and control.
Reliability, Maintainability, and Availability (RMA)	Quantitative and qualitative analyses of the attributes to optimize the RMA performance of a system within the program's operational and programmatic constraints throughout the system lifecycle. Qualitative analyses are in the form of failure mode assessments. Evaluation of the design's ability to meet operational readiness requirements through preventive and corrective maintenance.
Human Factors Engineering (HFE)	Human factors is a multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to: <ul style="list-style-type: none"> <li>– equipment, systems, facilities</li> <li>– procedures, jobs, environments</li> <li>– staffing</li> <li>– training</li> <li>– personnel and organizational management for safe, comfortable, and effective human performance.</li> </ul>

Specialty Engineering Discipline	Description
Electromagnetic Environmental Effects (E <sup>3</sup> )	Analysis of the system for susceptibility and/or vulnerability to electromagnetic fields or capability to generate such fields that might interfere with other systems and to identify sources of interference and means for correction within the levels prescribed by law, program requirements, spectrum management, or recognized standards. E <sup>3</sup> is composed of Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC)
Quality Engineering (QE)	An objective analysis of all planned and systematic activities to ensure that a product or service fulfills requirements and is of the highest quality.
Information Security Engineering (ISE)	Evaluation of the vulnerability of the system to unauthorized access and use or susceptibility to sabotage. Assessment of the ability of the system to survive a security threat in the expected operational environment.
Hazardous Materials Management/Environmental Engineering	Determination of environmental impacts at deployment sites and during operations, including both environmental impacts on the system and system impacts on the environment during all phases of the product life.

#### 4.1.2.8.3 Value

Specialty Engineering outputs are often used to validate and/or verify requirements and support technical decision on a program. In addition, change proposal documentation is produced if the conclusions of the analysis call for a revision to the Requirements or design baseline.

These analyses are used to support functional analysis (Section 4.4); define, allocate, and validate requirements (Section 4.3); contribute to the design (Section 4.5); and to evaluate design progress, technical soundness, and risk. Stakeholders also need them to ensure that the product performs as intended (Section 4.12), and engineering, operations, and product support personnel need them to accomplish their responsibilities in product development and operation.

These analyses help the program to define requirements and design features and/or describe characteristics of the design and related operations in support of Validation and Verification (Section 4.12), Requirements Management (Section 4.3), Trade Studies (Section 4.6), Synthesis (Section 4.5), and Functional Analysis (Section 4.4).

#### 4.1.2.9 Integrity of Analyses

[SEM 4.9; iCMM PA N/A]

##### 4.1.2.9.1 Objective

The Integrity of Analyses element (Section 4.9) seeks to provide systematic guidance that leads to analysis results that are credible, useful, sufficient, and verifiable.

#### 4.1.2.9.2 Definition

Analysis is defined as a logical examination or study of a system to determine the nature, relationships, and interaction of its parts and environment.

Integrity of Analyses is defined as 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.

#### 4.1.2.9.3 Value

Analyses are constantly being performed throughout SE and the program's lifecycle. These analyses range from simple to complex, quantitative to qualitative, top-down to bottom-up, and basic formulas to sophisticated simulations. To ensure credible, useful, sufficient, and timely data/results for program and/or technical decisions, the integrity and fidelity of the various analysis tools shall be understood and validated. This validation takes several forms: the attributes of the tool suite, validity of the input data, and proficiency and workmanship of the analyst. An Analysis Management Plan is generated that outlines the details of the various analysis methods and tools. It is recommended that this plan also reflect the program's constraints regarding technical capabilities, schedule requirements, and cost requirements.

The initial selection of the method, tools, or model to be used in an analysis focuses on determining a practical tool that provides the most visibility into the problem with the least complexity. Because this process is iterative, there is an ongoing need to use the best approach to select the right method, tool, or model, considering the preferences of the stakeholders, other teams' previous experience with different tools, and the limitations of budgets, technology, and schedule.

The bottom line is to have analyses in place that guard against mistakes and embed a consistent level of confidence in the integrity of the analysis. The analysis, in turn, contributes significantly to the success of the decision-making processes of program management, teams, stakeholders, and contract managers.

#### 4.1.2.10 Risk Management

[SEM 4.10; iCMM PA 13, 14, 18]

##### 4.1.2.10.1 Objective

The Risk Management element (Section 4.10) seeks to identify and analyze the uncertainties of achieving program or organizational objectives and develop plans to reduce the likelihood and/or consequences of those uncertainties.

Four lower level objectives are:

- Timely identification of risks (identifying a potential problem, with sufficient lead time so that the team may implement appropriate alternate plans)
- Consistent assessment of the level of risk across a program (providing a structured decision-making framework for prioritizing resource application)

- Communication of risk mitigation actions across the program/organization (ensuring that all elements of the program/organization are aligned in resolving risks)
- Review of risk mitigation action performance

#### **4.1.2.10.2 Definition**

Risk Management is 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.

Risk is defined as 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.

Risk Management seeks to understand and avoid the potential cost, schedule, and performance/technical risks to a project, and to take a proactive and well-planned role in anticipating them and responding to them if they occur. Risk Management is equally at home in project management as well as System Engineering because both domains have a common view of seeking out opportunities to solve a problem or fulfill a need. Opportunity represents the potential for improving value in achieving a goal; risk represents the potential for decreasing the same value. Hence, any discussion of Risk Management should include opportunity management. The methodologies, decision parameters, and outcomes apply as well to risks as they do to opportunities.

#### **4.1.2.10.3 Value**

Understanding the levels of likelihood and consequences of risk occurring increases the program manager's and program team's ability to anticipate and control the impacts of internal and/or external events on their programs. These impacts include, but are not limited to, cost, quality, schedule, and stakeholder satisfaction trends. The comprehensiveness of the analysis drives the thoroughness of what resources are required to mitigate the risk (e.g., budgets, requirements changes, stakeholder interfaces). Risk identification worksheets, tools, and terminology ensure a consistent approach that generates an analysis in which subjectivity is minimized, and confidence in the analysis is maximized.

#### **4.1.2.11 Configuration Management**

[SEM 4.11; iCMM PA 16]

##### **4.1.2.11.1 Objective**

The Configuration Management element (Section 4.11) seeks to establish and maintain consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.

#### 4.1.2.11.2 Definition

Configuration Management (CM) is defined as “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.”<sup>2</sup> The discipline provides a structured approach to identify, control, and maintain the configuration of a system/product during its lifecycle through establishment of baselines. 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. CM enables organizations to ensure the integrity of their products through all lifecycle phases.

The tasks focus on consistency of requirements, design, and operational information throughout the product’s life. Once baselined as defined by stakeholder requirements, changes are systematically approved and managed to ensure that traceability/accountability is maintained throughout myriad levels of documentation. The planning and execution of CM includes five fundamental practices: (1) plan CM process, (2) identify baseline elements, (3) manage approved baseline elements, (4) provide configuration status accounting, and (5) verify and audit configuration.

#### 4.1.2.11.3 Value

Configuration Management benefits the program, stakeholders, and contractors/suppliers. The discipline provides a structured approach to identify, control, and maintain the configuration of a system/product during its lifecycle through establishment of baselines. CM enables organizations to ensure product integrity through all lifecycle phases. As product attributes are defined, measurable performance parameters may be established for the product’s acquisition and use. As changes are made, Configuration Management provides correct and current information to the decision-making process. When configurations are managed, product repeatability is enhanced, guesswork and downstream surprises are avoided, cost and schedule savings are realized, erratic changes are minimized, proper replacement and repairs are ensured, and maintenance costs are reduced. The overall effect is establishment of a high level of confidence in the product information.

#### 4.1.2.12 Validation and Verification

[SEM 4.12; iCMM PA 08]

##### 4.1.2.12.1 Objective

The Validation and Verification element (Section 4.12) seeks to determine that the system and process requirements are correct and have been met.

Validation is performed to ensure the correctness and completeness of the requirements that define a solution. The objectives of the Validation process include:

- Developing the Validation Table and inclusion of the Validation Table in a Validation Report

---

<sup>2</sup> ANSI/EIA-649-1998, National Consensus Standard for Configuration Management.

- Appending to or referencing by the existing requirements documents of the Validation Report
- Confirming that the system services required are properly documented in the program requirements
- Confirming that the requirements resulting from the service-level gap analysis faithfully describe the required system functions.
- Reporting nonconformance, used to identify corrective actions
- Ensuring traceability of all requirements to the top-level program requirements
- Documenting the program's concerns and issues and constraints

Verification proves that a system is able to demonstrate (show evidence) that it complies with the Service Level Mission Need; functional, performance, allocated, derived, and interface requirements; and design and allocated constraints that provide the solution to the service gap analysis. The major objectives of the Verification process are:

- Intended functions are correctly implemented and that the system is operationally ready and acceptable to the users
- Requirements are satisfied
- Specialty Engineering analyses, including lifecycle, remain valid for the system as implemented

#### **4.1.2.12.2 Definition**

The Validation and Verification element ensures that all system requirements are correct and have been met. The Validation process proves that the right system is being built (i.e., that the requirements are unambiguous, correct, complete, consistent, operationally and technically feasible, and verifiable).

The Verification process ensures that the designed solution has met the system requirements and that the system is ready for use in the environment for which it is intended.

#### **4.1.2.12.3 Value**

The Validation process is conducted to provide objective evidence that the functionality of the solution, as defined in the program requirements, complies with the Service Level Mission Need. When variances are identified, they are recorded and used to guide corrective actions. Because Validation is a comparative assessment of the need and the requirements, it also confirms the service gap analysis.

The Verification process confirms that the development process has provided a solution that is consistent with stakeholder needs and compliant with the program's validated requirements. It is a basic principle to verify all requirements in the program requirements.

### **4.1.2.13 Lifecycle Engineering**

[SEM 4.13; iCMM PA 05, 09, 10, 12]

#### **4.1.2.13.1 Objective**

The Lifecycle Engineering (LCE) element (Section 4.13) seeks to meet the cost and performance objectives of a system during its entire lifecycle. Programs provide services that may be obtained from systems as well as systems of systems having multiple system elements (e.g., system of systems).

#### **4.1.2.13.2 Definition**

LCE objectively evaluates 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. The lifecycle includes the entire spectrum of activity for a given system, beginning with identification of a need and extending through a system design and development, production and construction, operational use, sustainment of support and system retirement, and, eventually, disposal.

#### **4.1.2.13.3 Value**

LCE manages costs from inception (cradle) to disposal (grave) for equipment and projects over their anticipated useful life span. LCE aims at providing an engineering discipline that provides best results when both art and science are merged with good judgment. These analyses are used to evaluate design progress, technical soundness, and risk. They are also needed by the stakeholders to ensure that the product performs as intended, as well as by engineering, operations, and product support personnel to accomplish their responsibilities in product development and operation.

### **4.1.2.14 System Engineering Process Management**

[SEM 4.14; iCMM PA 20 and 21]

#### **4.1.2.14.1 Objective**

The System Engineering Process Management element (Section 4.14) has three objectives:

- Maintain and improve SE processes contained in the SEM
- Train the workforce on the SE processes by managing the SE training materials and ensuring that they accurately reflect the processes described in the SEM
- Incorporate process innovation

#### **4.1.2.14.2 Definition**

System Engineering Process Management provides support and balance for the 12 other SE process elements. It also includes activities to measure and improve the SE process elements, which involve designing, developing, improving, and maintaining definitions of SE activities, work, products, methods, techniques, practices, and tools. It additionally provides the technology environment for developing systems and performing SE.

#### **4.1.2.14.3 Value**

This process provides the details and data to ensure and improve overall SE efficiency and effectiveness. In turn, improved SE reduces cost and schedule while improving NAS efficiency and safety.

## 4.2 Integrated Technical Planning

### 4.2.1 Introduction to Integrated Technical Planning

Planning determines in advance what tasks are needed to complete a project. A plan, as a minimum, contains the tasks to be done, when they need to be done, and who is responsible for accomplishing them. A plan is incomplete if it does not define the complementary physical and financial resources. **Integrated Technical Planning 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.**<sup>1</sup> Integrated Technical Planning provides the guidance and tools to track and manage program activity, as well as the program-specific process tailoring to optimally satisfy program needs.

This System Engineering (SE) element has two primary areas: (1) Plans and (2) Technical Monitoring and Control. The plans include the System Engineering Management Plan (SEMP); supporting technical plans (e.g., Master Verification Plan and the Lifecycle Plan); and the OMB Circular 15, Exhibit 300, Attachment 3, Implementation Strategy and Planning (ISAP) document. The Technical Monitoring and Control section discusses measurement, assessments, and quality gates (or milestones) designed to determine progress toward a successful project completion. This section includes guidance for all planning documents. Specific planning development details and templates are in Appendix E. Control and Monitoring development details and templates are in Appendix C.

Integrated Technical Planning applies to all programs/projects regardless of size, complexity, or program status (i.e., new or legacy). The size, complexity, and stage of the system lifecycle of a program determine 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 ISAP, SEMP, or other plans requires documentation only to the extent that existing plans don't support the changes.

In the Acquisition Management System (AMS), the Exhibit 300, Attachment 3, ISAP details the minimum program planning required. The ISAP includes the system implementation strategy, the programmatic planning, and a subset of SE planning.

In addition to the planning contained in the SEMP and ISAP, certain specialty domains require additional planning. For example, the NAS Modernization System Safety Management Plan governs system safety efforts conducted in the AMS and requires each program to develop an Integrated System Safety Program (ISSP) tailored to the program's safety needs. This is discussed in the Safety Management System (SMS) documentation on the FAA Acquisition System Toolset Web site.

---

<sup>1</sup> Visualizing Project Management: Models and Frameworks for Mastering Complex Systems (Hardcover) by [Kevin Forsberg](#), [Hal Mooz](#), [Howard Cotterman](#), John Wiley & Sons; 3rd edition, September 1, 2005, page 196.

#### **4.2.1.1 Integrated Technical Planning Objective**

Integrated Technical Planning provides program management a sound, repeatable plan for executing requirements-based programs in a structured manner.

#### **4.2.1.2 Process-Based Management**

The Process-Based Management (PBM) chart appears in Figure 4.2-1.

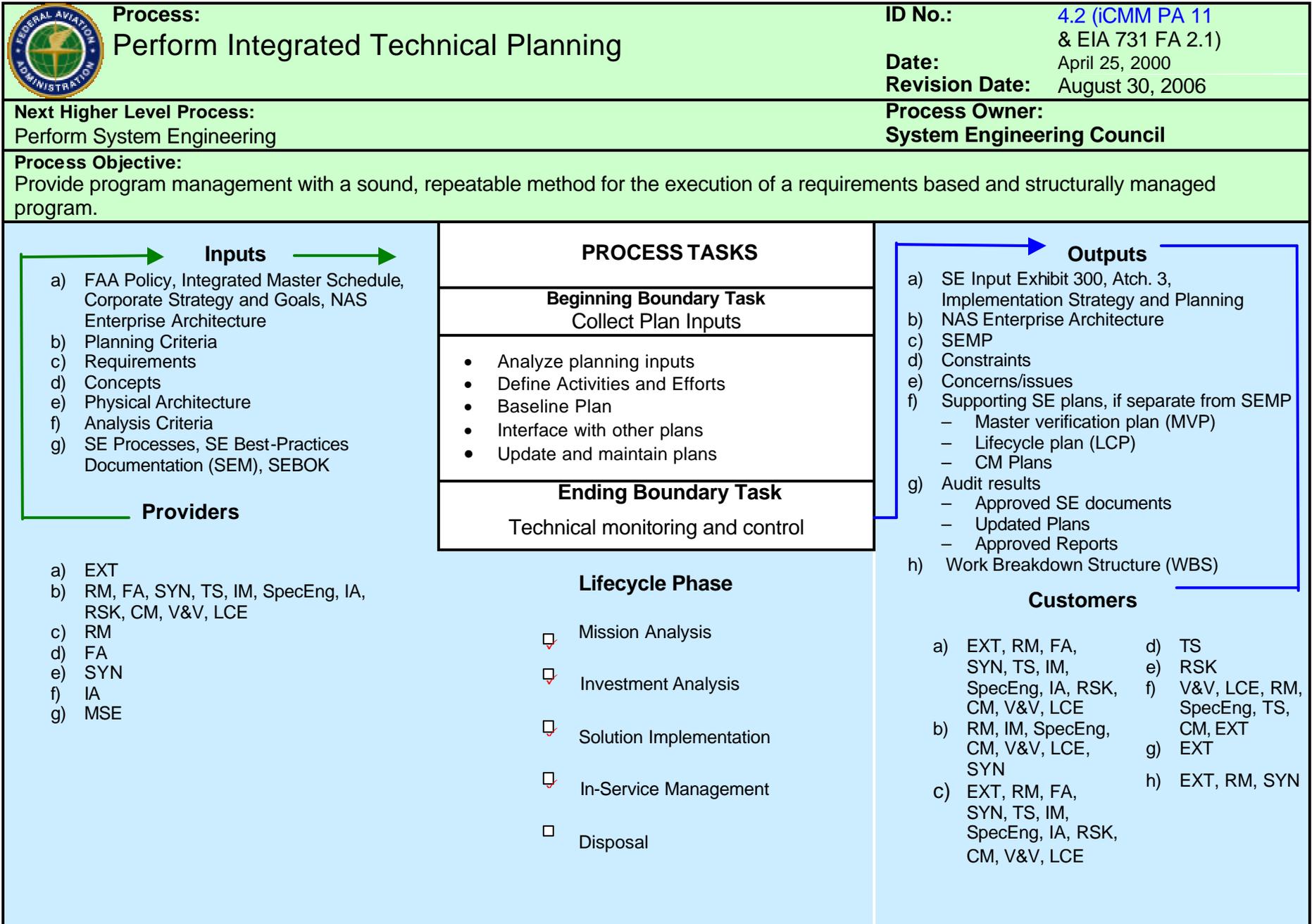


Figure 4.2-1. Integrated Technical Planning Process-Based Management Chart

### 4.2.1.3 Inputs to Integrated Technical Planning

The inputs to the process appear in the PBM chart. Although most inputs are internal to System Engineering, some are external (e.g., law, regulation, and policy).

FAA policy	Provides constraints and boundaries to planning
Integrated master schedule	Provides program milestones and associated dates to aid in developing completion dates for planned SE tasks
Corporate strategy and goals	Provides constraints and boundaries to planning
Planning criteria	Contains detailed information from other SE elements that defines scope of planning
Concept of operations	Describes how the system will be used including information on environment
NAS CONOPS	Describes how the system fits into the NAS
Analysis criteria	Ensures credible analysis results
Requirements	Bounds the Work Breakdown Structure (WBS)
FAA Enterprise Architecture	Describes the FAA enterprise architecture, of which the NAS Enterprise Architecture is an integral part

### 4.2.1.4 Outputs of Integrated Technical Planning

This table lists the outputs for this process.

SE Input to ISAP	Provides summarized planning for SE elements included in ISAP
NAS Enterprise Architecture	Describes the “as is” NAS and the planned future NAS
SEMP	Serves as primary SE planning document
Constraints	To other SE elements based on analyses performed during planning activities
Concerns and Issues	Provided to Risk Management for mitigation
Supporting SE Plans	Includes Master Verification Plan (MVP), Lifecycle Plan (LCP), Configuration Management (CM) Plan and other SE plans
From Technical Monitoring and Control	
Approved SE or Design Documents	Design-to-package, build-to-package, etc.
Updated Plans	Risk Management Plans, SEMP, LCP, Test plans, etc.
Approved Reports	Test, Technical Performance Measurement, Risk Management, etc.

### 4.2.1.5 Key Program Decisions

Key program decisions required for this process are:

- Request by stakeholders and/or program management for Integrated Technical Planning (usually included in the SEMP and ISAP)
- Identification of necessary planning elements by program system engineering and the project team
- Program management acceptance that the identified planning elements are necessary

- Baseline plan accepted by the program management, stakeholders, and Enterprise-level decision makers
- Program management's approval of the SEMP and ISAP and any other supporting technical plans (e.g., MVP and Lifecycle Plan (LCP))
- Enterprise-level approval of ISAP at final investment decision

#### **4.2.1.6 Key Process Interfaces**

Integrated Technical Planning interfaces with all other SE processes, either receiving inputs from them or providing outputs to them.

#### **4.2.1.7 Acquisition Management System Process Interface**

Chapter 3 describes the interface of the AMS process and SE milestones. AMS process activities that most strongly interact with SE must be considered in the Integrated Technical Planning process. All plans are living documents and are subject to continuous review and update to satisfy program needs and changes. All available plans should be reviewed at each AMS milestone and as part of subsequent system baseline modifications throughout the program lifecycle.

### **4.2.2 System Engineering Management Plan**

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. It identifies and ensures control of the overall SE process and provides greater SE implementation detail than the ISAP. The preliminary issue of the SEMP typically occurs in the first phase of Investment Analysis, with a completed version released for Final Investment Decision (formerly JRC 2b). A scheduled update occurs in System Implementation, with additional updates issued as necessary to reflect changing input conditions throughout the program/project.

#### **4.2.2.1 Inputs to System Engineering Management Plan**

The SEMP relates the technical requirements to program requirements, providing the structure to guide and control integration of engineering activities to achieve the SE objectives consistent with a top-level management plan for the program. The SEMP includes more detailed planning than the ISAP for all SE elements to be executed as part of the program. It helps execute the system development by defining the organizational structure; establishing the responsibilities, authority, and accountability of each; and clearly defining structural interfaces. It is recommended that this be an iterative process.

Information and data needed to begin preparing a SEMP include:

- Knowledge of corporate strategy and goals
- Description and understanding of the overall program/project, usually found in an ISAP (may be a draft)
- Identification of top-level program/project requirements, usually taken from the Service Level Mission Need (SLMN), Program Requirements, change requests, or one of the outputs developed during Mission Analysis
- Contract documents

- Any issues or constraints

#### **4.2.2.2 System Engineering Management Plan Steps**

The following steps shall be used to develop a SEMP.

##### **4.2.2.2.1 Step 1: Collect Inputs**

SEMP development relies on information from both technical and nontechnical documents. Inputs are also gathered from the Screening Information Request (SIR), Statement of Work (SOW), Integrated Master Schedule (IMS), and draft ISAP.

##### **4.2.2.2.2 Step 2: Analyze Inputs**

To determine the SE effort required and committed to by program management, review the ISAP that reflects the nature and magnitude of the program/project. For example:

- Large and complex system developments demand full SE application to ensure success
- Small-scale projects may be run under a subset process
- SE coordinates with the Service Organization, as its concurrence ensures compliance with the SEMP

##### **4.2.2.2.3 Step 3: Define Activities and Efforts**

After evaluating all inputs, determine how to integrate activities. Decisions that should be made involve:

- Tailoring the SE process
- Selecting an approach to ensure integration of engineering specialties
- Determining how program team members interact and communicate to execute technical program planning and control
- Identifying the explicit SE responsibilities, accountability, and authority, accounting for all planned tasks
- Developing the structure of the comprehensive SE inputs to the IMS (included in the ISAP) for scheduled tasks

##### **4.2.2.2.4 Step 4: Baseline**

Prepare a draft SEMP for review and comment, using input from all affected SE elements, enterprise management, and, when appropriate, the stakeholders. The draft may also include contractual SE requirements, such as a Contract Data Requirements List (CDRL) Item and/or Data Item Description, with which all affected parties shall comply.

##### **4.2.2.2.5 Step 5: Interface With Other Processes/Plans**

The SEMP interfaces with, and forms a roadmap to, any other SE and engineering specialty standalone plans (e.g., Master Verification Plan). The SEMP addresses all SE elements:

- Integrated Technical Planning (Section 4.2)

- Requirements Management (Section 4.3)
- Functional Analysis (Section 4.4)
- Synthesis (Section 4.5)
- Trade Studies (Section 4.6)
- Interface Management (Section 4.7)
- Specialty Engineering (Section 4.8)
- Integrity of Analyses (Section 4.9)
- Risk Management (Section 4.10)
- Configuration Management (Section 4.11)
- Validation and Verification (Section 4.12)
- Lifecycle Engineering (Section 4.13)
- System Engineering Process Management (Section 4.14)

**4.2.2.2.6 Step 6: Update and Maintain the Plan**

It is recommended that throughout the lifecycle of the program/project, SE monitors inputs (especially to the ISAP) and, when there is a significant change in one or more inputs, revises the SEMP (by repeating steps 1–5 above).

**4.2.2.3 System Engineering Management Plan**

Table 4.2-1 is a SEMP outline.

**Table 4.2-1. System Engineering Management Plan Outline**

SECTION 1	INTRODUCTION
1.1	Scope
1.2	Purpose of the System Engineering Management Plan
1.3	Organization of the System Engineering Management Plan
1.4	SEMP Overview
1.5	Program/Project Name, System Description, Scope, Status, and Life cycle stage (or segment)
1.6	Program Organization
1.7	System Engineering Responsibility Assignments
1.8	System Engineering Environment and Tools
1.9	System Engineering Metrics

**Table 4.2-1. System Engineering Management Plan Outline—Continued**

1.10	Applicable Documents
SECTION 2	SYSTEM ENGINEERING
2.1	System Engineering Process
2.2	Integrated Technical Planning
2.3	Requirements Management
2.3.1	Concept and Requirements Definition (system)
2.4	Functional Analysis
2.5	Synthesis
2.6	Trade Studies
2.7	Interface Management
2.7.1	Establish Interface Working Group
2.8	Specialty Engineering
2.8.1	System Safety Engineering
2.8.2	Human Factors Engineering (summarized in ISAP Section 17)
2.8.3	Quality Engineering (summarized in ISAP Section 5.2)
2.8.4	Reliability, Maintainability, and Availability
2.8.5	Electromagnetic Environmental Effects/Spectrum
2.8.6	Information System Security
2.8.7	Hazardous Materials Management/Environmental Engineering
2.9	Integrity of Analysis
2.10	Risk Management
2.11	Configuration Management (summarized in ISAP Section 9)
2.11.1	Data Management
2.11.2	Establish CCB
2.12	Validation and Verification (summarized in ISAP Section 12)
2.13	Lifecycle Engineering
2.13.1	Real Property Management
2.13.2	Deployment and Transition
2.13.3	Integrated Logistics Support
2.13.3.1	Maintenance Planning
2.13.3.2	Maintenance Support Facility
2.13.3.3	Direct-Work Maintenance Staffing
2.13.3.4	Supply Support

**Table 4.2-1. System Engineering Management Plan Outline—Continued**

2.13.3.5	Support Equipment
2.13.3.6	Training, Training Support, and Personnel Skills
2.13.3.7	Technical Data
2.13.3.8	Packaging, Handling, Storage, and Transportation
2.13.3.9	Computer Resources Support
2.13.4	Sustainment/Technology Evolution
2.13.4.1	Sustainment
2.13.4.2	Technology Evolution
2.13.5	Disposal
2.14	System Engineering Process Management
2.2	Master Verification Plan
2.21	Validation
2.22	Verification
SECTION 3	
3.1	System Engineering Master Schedule (use Program Integrated Master Schedule as guidance)
3.2	Reviews and Audits
3.3	Work Breakdown Structure

#### 4.2.2.3.1 SEMP Planning Details

The SEMP includes planning for all SE elements that the program requires, including specialty elements. The planning details for each SE element are in Appendix E. Some SE planning information in the SEMP will be summarized and inserted in the ISAP (see subsection 4.2.5 below).

The Work Breakdown Structure (WBS) is 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. Project components may be projects or services.<sup>2</sup> However, for highly time-dependent projects with organizational “checkpoints” or “gates” that allow for progress from phase to phase, the task-oriented WBS may be the most effective.<sup>3</sup> WBS numbering schema follows the functional analysis standard (see Functional Analysis (Section 4.4)), with the highest level being the project level and the lowest level being the work package.

<sup>2</sup> Guide to Project Management Body of Knowledge. PMI Standards Committee. Project Management Institute, PA, 1996.

<sup>3</sup> How to Build a Work Breakdown Structure, The Cornerstone of Project Management, Carl Prichard, ESI International, Arlington, VA 22203, 1998.

The WBS is an exhaustive, hierarchical (from general to specific) tree structure of deliverables and tasks that need to be performed to complete a project. The WBS identifies terminal elements (i.e., the actual items to be done in a project). Therefore, the WBS serves as the basis for much of project planning. An example of a work breakdown for painting a room (activity oriented) follows:

- Develop room-painting plan
- Prepare materials
  - Buy paint
  - Buy a ladder
  - Buy brushes/rollers
  - Buy wallpaper remover
- Prepare room
  - Remove old wallpaper
  - Remove detachable decorations
  - Cover windows with old newspapers
  - Cover outlets/switches with tape
  - Cover furniture with sheets
- Paint the room
- Clean up the room
  - Dispose or store leftover paint
  - Clean brushes/rollers
  - Dispose of old newspapers
  - Remove covers
  - Unpaint dog

The WBS provides the framework for organizing and managing work, including large, complex projects. It entails breaking the projects into progressively smaller pieces until they are a collection of defined "work packages" that may include a number of tasks. A \$1 billion project is simply a number of \$50,000 projects joined together. The size of the WBS should generally not exceed 100–200 terminal elements. If more terminal elements seem to be required, use subprojects.) The WBS should be at least three to four levels deep, with each level five to nine elements broad.



A WBS is not a "to do" list. Developing the WBS as such gives no foundation for clear assignments, close tracking, or tight scope control. This leads to a project taking about 50 percent longer than it should, as the team spends hours in status meetings discussing what to do next. It also leads to micromanagement.

For various programmatic reasons, any element in the SEMP may require a more detailed standalone plan (e.g., risk management plan, configuration management plan, or concept and requirement definition (CRD) plan). A plan must define the tasks and products of the process and assign responsibilities to various subprocesses. A plan must also describe the deliverables and include the schedule for completion of each task and delivery of each product. Sometimes, a SEMP element needs a separate plan. Details for these standalone plans (for each individual SE element) appear in Appendix E. The most likely to be standalone plans are the Master Verification Plan, the Lifecycle Plan, the Risk Management Plan; the Configuration Management Plan; the Concepts and Requirements Definition Plan, and the Program Safety Plan.

Appendix E also contains detailed input and format information for the planning associated with all of the SE elements discussed in Section 2 of the SEMP (as in the outline above.)

### **4.2.3 Verification Planning**

Although verification planning may be contained in the SEMP, it is most often a standalone MVP, which contains validation and verification planning as well as test and evaluation planning. (See Section 4.12, Validation and Verification, for definitions of these terms.) This plan includes all the activities to ensure that the right system is being built and to confirm that evolving system solutions comply with functional, performance, and design requirements, as well as performance and characteristics of the delivered system. Validation activities dominate the early phases of the lifecycle, while verification activities dominate the later phases. The MVP defines all validation and verification activities that demonstrate the system's capability. Details for a standalone MVP appear in Appendix E.

### **4.2.4 Lifecycle Planning**

Although the lifecycle planning may be included in the SEMP, it is usually a separate LCP. In either case, the plan (or planning section) describes the tasks to perform lifecycle 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, Deployment and Transition, Real Property Management, Sustainment and Technology Evolution, and Disposal. The Integrated Logistics Planning section includes these subsections: maintenance; maintenance support facilities; 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. The format for a standalone LCP is in Appendix E.

#### **4.2.4.1 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. Detailed information on these activities is in Appendix E (13.1).

#### **4.2.4.2 Deployment and Transition**

This section includes all tasks to prepare for and assess the readiness of a solution to be implemented into the National Airspace System (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.

#### **4.2.4.3 Real Property Management**

This section includes resources to determine if real property is required, acquisition costs, and acquisition strategy (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.

#### **4.2.4.4 Sustainment and Technology Evolution**

This section shall include 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 [c1]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
  - Supporting revalidation or development of SLMN

#### **4.2.4.5 Disposal**

This section shall include all activities associated with disposal management; dismantling/demolition/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.

#### 4.2.5 Exhibit 300, Attachment 3, ISAP

The ISAP 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. A draft ISAP is completed before the Initial Investment Decision milestone, and the final ISAP is approved at the Final Investment Decision. The ISAP is reviewed and updated at all subsequent SE and acquisition reviews and reflects changes throughout the program’s lifecycle.

##### 4.2.5.1 Introduction to Exhibit 300, Attachment 3, ISAP

The ISAP is the recognized plan used to manage a project and contains the program Integrated Master Schedule, which includes milestones (events), accomplishments, and criteria. The ISAP relates tasks to program events and demonstrates a logical, event-driven sequence of effort. It is directly traceable to the WBS, which is produced and owned by SE, and the SOW. The ISAP provides vertical and horizontal task integration through its task statements and numbering system and identifies task relationships. It 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. The ISAP establishes contractual requirements and unique programmatic requirements. The planning elements in the tailored SEMP will be summarized in the ISAP to ensure that ALL planning is referenced in the ISAP. Table 4.2-2 lists the sections of an ISAP with the associated SEM section referenced where applicable. The planning content for these SE elements will be a summarized extract from the SEMP to ensure consistency.



Although the ISAP reflects selected SEMP planning elements, complete SE planning content is in the SEMP (or subordinate planning documents). Additional SE planning beyond that mandated in the ISAP ensures a more accurate costing of the program and a higher likelihood of success. Performance of these planned elements will significantly reduce the percentage of requirements found in Operational Test and Evaluation. Although this additional SE planning can be included in the ISAP at a summary level, it must be included in depth in the SEMP.

**Table 4.2-2. Implementation Strategy and Planning Table of Contents**

1	BACKGROUND
1.1	Mission Need (See SEM 4.3)
1.2	Status
2	OVERVIEW
2.1	Description

**Table 4.2-2. Implementation Strategy and Planning Table of Contents—  
 Continued**

2.2	Objectives and Capabilities
2.3	Key Elements
2.4	Deliverables
3	INTEGRATED PROGRAM SCHEDULE
4	PROGRAM STRATEGY
5	MANAGEMENT STRATEGY
5.1	Management Team
5.2	Program Control and Quality Assurance
5.3	Contract Management
5.4	Requirements Management
5.5	System Safety Management (frequently a separate plan — SSMP)
6	PROCUREMENT STRATEGY
6.1	Sources
6.2	Source Selection
6.3	Competition
6.4	Contract Type
6.5	Government Furnished Property and Information
6.6	Warranties and Data Rights
7	BENEFITS AND PERFORMANCE
8	SYSTEM ENGINEERING—includes SEMP elements not listed elsewhere in ISAP (at the summary level with details in SEMP)
9	CONFIGURATION MANAGEMENT (See SEM 4.11)
10	SECURITY AND PRIVACY
10.1	Physical Security
10.2	Information Security (See SEM 4.8.6)
10.3	Personnel Security
10.4	Privacy
11	HARDWARE AND SOFTWARE DEVELOPMENT (see SEMP)
12	TEST AND EVALUATION (includes the MASTER VERIFICATION PLAN) (See SEM 4.12)
12.1	Test Strategy Overview
12.2	System Test
12.3	Independent Operational Test and Evaluation
12.4	Field Familiarization Test

Table 4.2-2. Implementation Strategy and Planning Table of Contents—Continued

12.5	Master Verification Plan
13	PRODUCTION
14	FACILITIES
15	PHYSICAL INTEGRATION (See SEM 4.13)
15.1	Real Property
15.2	Environmental Requirements
15.3	Energy Conservation
15.4	Heating, Ventilation, and Air-Conditioning
15.5	Grounding, Bonding, Shielding, and Lightning Protection
15.6	Cables
15.7	Hazardous Materials (See SEM 4.8.3)
15.8	Power Systems and Commercial Power
15.9	Telecommunications
15.10	Special Considerations
16	FUNCTIONAL INTEGRATION (See SEM 4.4)
16.1	Integration With Other NAS and Non-NAS Elements
16.2	Software Integration
16.3	Spectrum Management (See SEM 4.8.4)
16.4	Standardization
17	HUMAN INTEGRATION (See SEM 4.8.2)
17.1	Human/Product Integration
17.2	Employee Health and Safety
17.3	Specialized Skills and Capabilities
18	INTEGRATED LOGISTICS SUPPORT (See SEM 4.13)
18.1	Staffing
18.2	Supply Support
18.3	Support Facilities and Equipment
18.4	Technical Data
18.5	Training and Training Support
18.6	First and Second Level Repair
18.7	Packaging, Handling, Storage, and Transportation
19	DEPLOYMENT
20	IN-SERVICE MANAGEMENT
21	SUPPORTING SE PLANS
21.1	MASTER VERIFICATION PLAN
221	INTEGRATED LIFECYCLE PLAN (SE lifecycle elements not contained in 15 and 18 above)

#### 4.2.5.2 Inputs to Attachment 3, Implementation Strategy and Planning

The following inputs are necessary to develop the ISAP:

- Program objective as reflected in the Service-level Mission Need (SLMN) and Exhibit 300, Attachment 1, Program Requirements, which detail the operational environments in which the system is expected to operate
- Program-specific guidelines
- Top-level program constraints and assumptions, including program-specific organizational constraints and assumptions to be used on the program
- Program-specific schedule constraints and events
- Concept approach, including top-level conceptual alternatives, functional analyses, design support alternatives, and initial system evaluations
- Investment (or program) WBS
- Any specified government or external standards to be employed in the program
- Any other supporting technical plans (e.g., MVP and SEMP) to be presented at the Final Investment Decision

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.

#### 4.2.5.3 Implementation Strategy and Planning Steps

An ISAP is the responsibility of program management, who may delegate the writing and coordinating to SE. The ISAP is developed using the same basic planning steps used in developing the SEMP (see subsection 4.2.2.2 above).

#### 4.2.5.4 Implementation Strategy and Planning

#### 4.2.5.5 Integrated Technical Planning Inputs to the Implementation Strategy and Planning (Attachment 3 to Exhibit 300)

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 ISAP. 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, MVP, RMP, 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 ISAP will be included at a summary level in the SE management planning section of the ISAP, with the details in the SEMP. All ISAP 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 ISAP sections or tailoring any process must be documented, and the program manager must approve these actions. It is recommended that, as part of the ISAP, these planning sections be reviewed and changed whenever dictated by a change in the program or discovery of a discrepancy in the ISAP. 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. Table 4.2-3 lists the sections of an ISAP and the SE elements from the SEMP that provide summary-level inputs to the applicable ISAP sections with a brief textual explanation of each entry after the table. The ISAP summarizes SE activities, while the SEMP and other supporting technical plans describe the implementation detail.

**Table 4.2-3. SE Inputs to the Exhibit 300, Attachment 3**

Implementation Strategy and Planning		System Engineering Element
1	BACKGROUND	
1.1	Mission Need	Requirements Management
1.2	Status	Integrated Technical Planning (ITP)
2	OVERVIEW	
2.1	Program Scope	ITP
2.2	Products	ITP
3	INTEGRATED PROGRAM FUNDING	EXTERNAL
	INTEGRATED PROGRAM SCHEDULE	ITP
5	PERFORMANCE	
5.1	Core Work Activities	ITP; Functional Analysis (FA); Synthesis (SYN); Trade Studies (TS); Interface Management (IM); Integrity of Analyses (IA); Specialty Engineering (SpecEng) — Reliability, Maintainability, and Availability (RMA) and Quality Engineering))
5.2	Program Management Work Activities	Requirements Management (RM); SpecEng (System Safety); Risk Management (RSK); Technical Monitoring and Control (ITP)
5.3	Procurement Work Activities	ITP
6	BENEFITS	RM, RSK, LCE
7	PHYSICAL INTEGRATION	Lifecycle Engineering (LCE — real property; deployment and transition); SpecEng (Hazardous Materials Management/Environmental Engineering and Electromagnetic Environmental Effects (E <sup>3</sup> ))
8	FUNCTIONAL INTEGRATION	IM
9	HUMAN INTEGRATION	SpecEng (Human Factors Engineering)
10	SECURITY	SpecEng (Information Security Engineering)
11	SAFETY	SpecEng (Safety)
12	IN-SERVICE SUPPORT	LCE (Integrated Logistics Support; Sustainment/Technology Evolution)

Implementation Strategy and Planning		System Engineering Element
13	VALIDATION (INCLUDES TEST AND EVALUATION) AND MASTER VERIFICATION PLAN	Validation and Verification (V&V)
14	IMPLEMENTATION AND TRANSITION	LCE (Deployment and Transition; Disposal)
15	QUALITY ASSURANCE	SpecEng (Quality Engineering)
16	CONFIGURATION MANAGEMENT	Configuration Management (CM)
17	IN-SERVICE MANAGEMENT	LCE (Integrated Logistics Support (ILS); Sustainment/Technology Evolution)
18	SYSTEM ENGINEERING MANAGEMENT PLAN	ITP, FA, RM, SYN, TS, IA, RSK, IM, SpecEng,
19	LIFECYCLE PLAN	LCE
20	MASTER VERIFICATION PLAN	V&V

#### 4.2.5.5.1 Background

Integrated Technical Planning (ITP) is the source of information for summarizing the mission need and program status.

#### 4.2.5.5.2 Overview

ITP is the source of information about the scope of the program and the primary deliverables.

#### 4.2.5.5.3 Integrated Program Funding

ITP is the source for WBS, level-of-effort, and schedule/duration information in sufficient detail to enable cost estimators to identify funding requirements.

#### 4.2.5.5.4 Integrated Program Schedule

ITP is the source for WBS, milestone, and SE activity information to allow for a logical networking of program activities to achieve program objectives.

#### 4.2.5.5.5 Performance

The Performance section of the ISAP contains planning information on the “Core Work Activities,” the “Program Management Work Activities,” and the Procurement Work Activities. The “Core Work Activities” describes SE elements that are not specifically broken out as separate work activities. SE elements such as Integrated Technical Planning, Functional Analysis, Synthesis, Trade Studies, Interface Management, Integrity of Analyses, and Specialty Engineering sub-elements—including Electromagnetic Environmental Effects and Reliability, Maintainability, and Availability—can be addressed to the extent that they apply. The “Program Management Work Activities” identifies specific SE elements such as Requirements Management, Specialty Engineering (e.g., System Safety), and Risk Management as work activities requiring discussion. It also describes Program monitoring and control (including metrics), with Integrated Technical Planning as the source. The “Procurement Work Activity” identifies those SE resources required to support Screening Information Request (SIR) release,

Request for Proposal development, proposal evaluations, and contractor requirements definition.

#### **4.2.5.5.6 Benefits**

Requirements Management is the source for technical or performance benefits. Risk Management is the source of the risks incurred in pursuing these benefits.

#### **4.2.5.5.7 Physical Integration**

SE inputs to this ISAP section identify activities (e.g., space, facility, environment, power, and hazardous materials) that require planning.

#### **4.2.5.5.8 Functional Integration**

SE inputs to this ISAP section include planning for function analyses to identify functions needed to perform system tasks and development of a functional architecture.

#### **4.2.5.5.9 Human Integration**

SE inputs to this ISAP section include the individual human factors engineering work tasks that must be done during program implementation. For each task, the ISAP assigns the responsible individual and organization, identifies any output and the approval authority, specifies when the task should be completed, and allocates resources.

#### **4.2.5.5.10 Security**

SE inputs to this ISAP section include tasks to ensure that security is fully integrated into the system. The section addresses the key physical and information security tasks, including identifying security requirements, assessing system alternatives and analyzing security risks, and evaluating security features and controls for continuity of operations and disaster response to ensure appropriate availability.

#### **4.2.5.5.11 Safety**

SE inputs to this ISAP section include tasks needed to ensure that safety is fully integrated into the system.

#### **4.2.5.5.12 In-Service Support**

The preliminary In-Service Decision (ISD) activities of the deployment planning process focus on preparing for the ISD meeting. The post-ISD activities focus on documenting the ISD, establishing a periodic review, and tracking progress of completing the ISD Action Plan.

#### **4.2.5.5.13 Verification**

See the SEMP (Section 4.2.2) and MVP (subsection 4.2.3 above).

#### **4.2.5.5.14 Implementation and Transition**

This ISAP 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.

#### **4.2.5.5.15 Quality Assurance**

This ISAP planning section includes developing high-level quality requirements, providing constraints for risk management, and identifying development and deployment metrics. The quality assurance planning also includes supporting contract activities by providing evaluation criteria, assisting in estimating cost, and evaluating proposals.

#### **4.2.5.5.16 Configuration Management**

This ISAP section includes the CM tasks for ensuring that CM is performed throughout the lifecycle and for all aspects of the program.

#### **4.2.5.5.17 In-Service Management**

This ISAP section includes maintenance, staffing, supply support, support equipment, computer resources, training, and required personnel skills.

#### **4.2.5.6 Concept and Requirements Definition Plan**

Another plan that AMS requires is the concept and requirements definition plan. This plan specifies the scope, assumptions, constraints, methods, data sources, resources, control strategy, team composition, roles and responsibilities, schedule, and deliverables for a CRD activity that addresses a priority service need within the Service-Level Mission Need and develops the information necessary for an Investment Analysis Readiness Decision (IARD). Specifics on this plan are in Appendix E (E.11).

#### **4.2.6 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 manages the progress of the technical aspects of a system development or deployment. This topic includes both techniques and mechanisms to help ensure that results happen as planned and that unplanned results don't happen. In other words, it measures or assesses progress against a plan, identifies variances, and provides sufficient information for informed decision making on corrective action(s) 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. Several management tools and techniques are available to manage the program, mainly in the area of cost (resources) and schedule (time). An example of this approach is the application of Earned Value Management (EVM) to measure and analyze the cost and schedule performance of an investment program. While these measures may differ in their focus (technical versus nontechnical), they share a common basis of reference: the WBS.

The control aspect of the process is accomplished through 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 that contribute to the eventual realization of program objectives.

Each technical review or audit establishes the readiness of a program to proceed to the next phase of the system's lifecycle. Typically, they focus on the development phases, where SE provides the largest benefit to the investment. 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. Technical reviews employ specific criteria tailored to each phase of the lifecycle. These criteria verify the extent of technical progress made toward solving the identified capabilities shortfall.

Certain reviews and audits directly support an AMS phase exit decision point. Others provide interim benchmarks on the progress and maturity of the effort associated with the given phase. The reviews and audits are shown in Figure 4.2-2, which contains the same information as Figure 3.3-1 (see Chapter 3), and are grouped by the FAA AMS phase and decision points they support. Each SE milestone in Figure 4.2-2 is summarized in subsection 4.2.6.2.3 along with its objectives and scope related to the lifecycle phase it is supporting. Further details on each milestone are found in Appendix C and include an expanded discussion tailored to each milestone, including entry/exit criteria, process steps, and preparation checklists where appropriate. For the purposes of this SEM, the AMS lifecycle phases and their related reviews and audits are shown in Figure 4.2-2, which is based on the AMS policy as of November 2005.

# Product Planning & Development Process

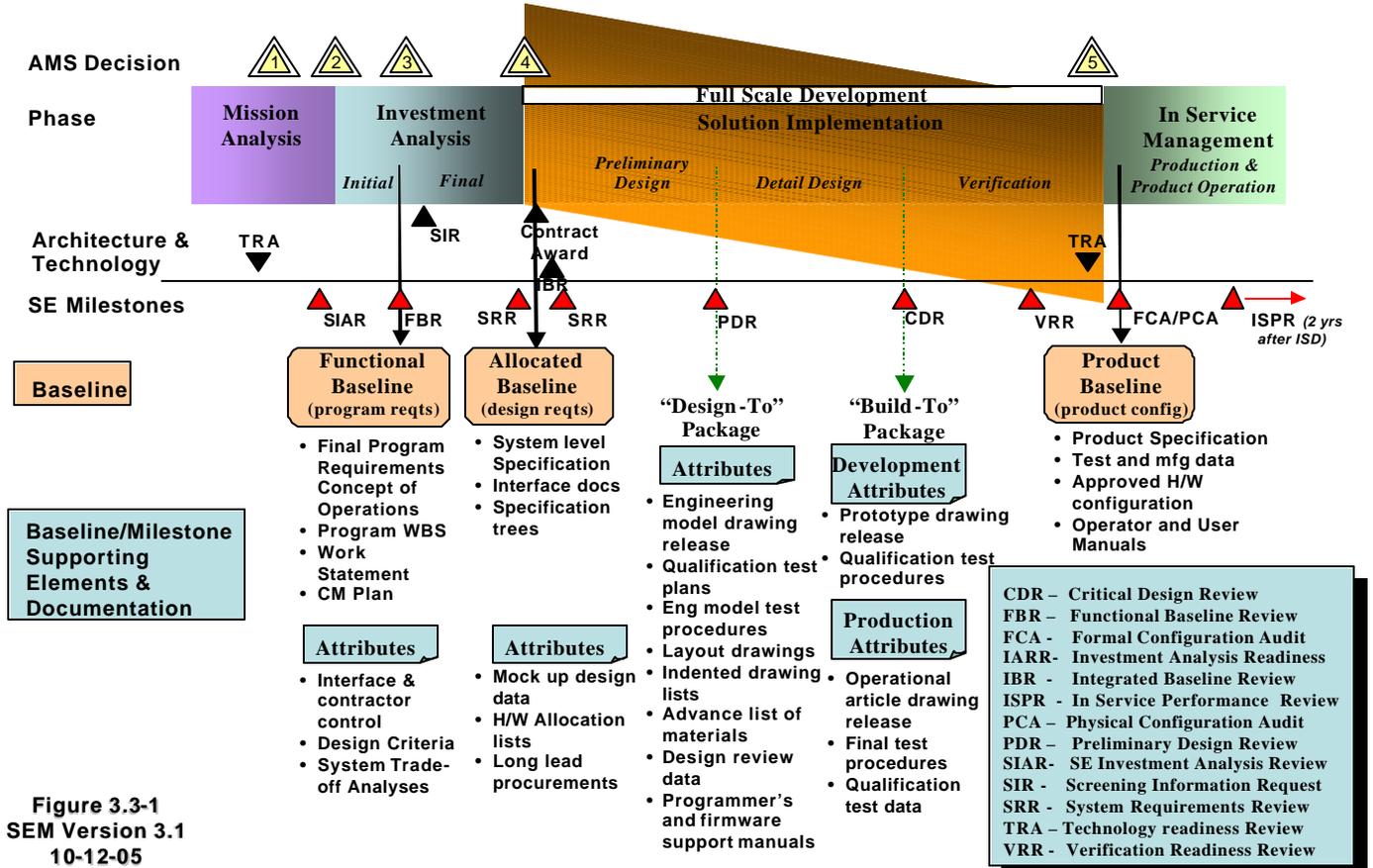


Figure 3.3-1  
SEM Version 3.1  
10-12-05

Figure 4.2-2 Product Planning and Development Process

## 4.2.6.1 Technical Measurement

Technical Performance Measurement (TPM) is the key technique used in monitoring and assessing technical progress throughout 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 preestablished 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.

The parameters used in a TPM program are called Technical Performance Parameters (TPP). 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 TPPs over time toward the desired value at completion of development. The projection can be based on verification, validation, planning or historical data. Not all TPPs are created equal. A subset of the TPPs characterizes the significant total system performance qualities, sometimes referred to as Key Performance Parameters (KPP), or simply “design drivers.” The critical requirements are either selected or derived from Measures of Effectiveness (MOE), which reflect operational or performance requirements, usually from the preliminary Program Requirements (pPR). These should be identified as part of the exit criteria for the Mission Analysis phase, usually as an outcome of the Investment Analysis Readiness Review (IARR). The balance of the TPPs are established during the Investment Analysis phase. These TPPs are revised and refined when the final Program Requirements (fPR) is finalized and could be further expanded or refined as the specific solution takes shape.



**In selecting a TPP, a critical performance value or limit is identified. This represents the absolute limit for the final as-built design. For the purposes of minimizing technical risk associated with the TPP, a target performance value is established that is within the critical performance limit and that provides a contingency or reserve to cover unexpected design problems and changes. The values of the parameter between this target value and the critical limit can be divided into ranges with different associated risk levels as shown in Figure 4.2-3. As the design progresses, the value of the TPP at completion is projected based on the current state of the design. As the design approaches completion and realization, the projected value of the TPP will converge to the final as-built design value. Accurate projections of the TPP along with trend analysis will help identify risks and provide opportunities to mitigate those risks more efficiently and effectively. A properly selected TPP should exhibit the following characteristics:**

- **Stated as quantifiable requirements in specification(s)**
- **Assessable through engineering analysis**
- **Can be verified by test and analysis**

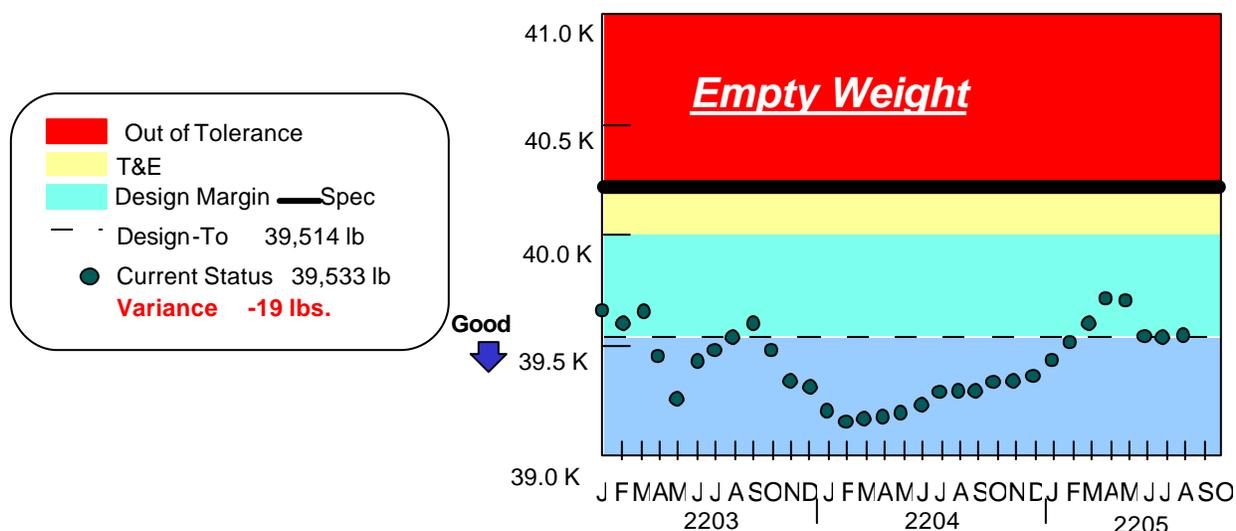


Figure 4.2-3. TPM Status Example

An effective TPM program provides an early warning regarding the adequacy of a design in terms of satisfying selected key performance parameter requirements of a system or end product. TPM examines marginal cost benefit of performance in excess of requirements. It also includes sensitivity analysis. Successful use of TPMs on the project includes:

- Identifying the technical performance measures that will be used to determine the success of the system, or portion thereof, and that will receive management focus and be tracked using TPM procedures. This would include incremental measures taken to assess the probability of meeting the objectives. It could include specific measures to determine reliability, maintainability, availability, testability, safety, electromagnetic properties, weight, balance, and manufacturability.
- Defining product and process metrics. These include: (1) product metrics to evaluate the quality of the product; (2) process metrics to evaluate efficiency and effectiveness of the tasks of the technical effort; and (3) frequency and methods to collect product and process metrics.



**The linkage between a critical requirement and the TPP is often overlooked or forgotten over time. Requirements are changed to fit the evolving needs of the project, and the link to the TPP is often broken. A simple technique to maintain the linkage between the originating requirement and the associated TPP is to visually highlight that linkage directly in the requirements document. This can be done by bolding the requirement, putting it in italics, or otherwise annotating the association.**

Project metrics are measures that both the project manager and the systems engineer use to track and monitor the project and the expected technical performance of the system's development effort. Identifying and monitoring metrics are important so that the team can determine if the project is "on-track" both programmatically and technically. For project metrics, the analog to TPM is Program Performance Measurement (PPM). This is a process used to track the current status of meeting selected Program Performance Requirements. The

nontechnical equivalent to TPPs are Program Performance Parameters (PPP). Figure 4.2-4 shows examples of TPPs and PPPs for an aircraft design and manufacturing program.

The most common application of PPM is the use of Earned Value Management (EVM). To objectively define the program baseline cost objectives and track them against performance and schedule, an EVM system is established. Earned Value is a management technique for integrating cost, schedule, technical performance measurement, and risk management.

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. ANSI/EIA-748 is the industrywide standard for a viable EVM system.

Technical Performance Parameter (TPP)	Specification Value	Program Performance Parameter (PPP)	Target Value (Examples)
Weight Empty		<b>(Program Performance)</b>	
Return Payload		Personnel Skill/Staffing Level	100% (Plan)
Specific Thrust		Drawing Release/Change Status	+/- (Schedule)
Avg Production Airframe/Contractor – Furnished Equipment (CFE) Cost		Quality Indicators	< x % change
ILS Airframe/CFE Cost		Organization/Counterparts	% match
Operating and Support Cost		Shortages	< x %
Detection range		Tools/Parts Fabricated	+/- (Schedule)
Thermal Management — Heat		Action Tracking System	# open, # days
Reliability		CDRL Status	# late/in review
Maintainability		Schedule Performance Index (SPI) and Cost Performance Index (CPI)	Percentage

Growth Provisions — Volume			
Growth Provisions — Electrical			<b>(Risk Trend Indicators)</b>
Growth Provisions — Liquid Cooling		90 Day Look Ahead	# realized
False Alarm Rate		High Risk Items	# active
Fault Detection		Mitigation Plans	# Unapproved
Fault Isolation		Transition to Production	# Open areas
Central Processing Unit (CPU) Throughput		Overall Program Risk Status	Profile (trend)

**Figure 4.2-4. Performance Measures (Aircraft Manufacturing Example)**

#### 4.2.6.2 Technical Controls

Control gates are formal decision points along the lifecycle that the system owner and stakeholders use 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. 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 System Engineering control gates (or milestones) in Figure 4.2-2 (above) are typically in the form of technical reviews or audits.

##### 4.2.6.2.1 Technical Reviews

Technical reviews assess the maturity of the product or service under consideration. While the mandatory reviews are identified in the following subsections, additional reviews can be performed based on the program’s specific needs. Technical reviews, which are scheduled at strategic points within the development cycle, employ specific criteria tailored to the development effort. These criteria verify the extent of technical progress made toward solving the identified capabilities shortfall.

Figure 4.2-2 discusses the relationship of the technical reviews and the AMS phases. In the Mission Analysis and Investment Analysis phases, the goal is to ensure that the definitions of the need and its derived operational requirements are complete and accurate and that all design constraints have been identified. In the Solution Implementation phase, the goal is to monitor the technical progress of the development to ensure that it remains consistent with the established operational requirements and design constraints. An additional goal during Solution Implementation is to assist program management to assess the maturity of the design in order to identify risks and form the basis for determining overall progress in the program.



**In each case, a well-structured technical review includes defined entry criteria (inputs for conducting a successful review), 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.**

All technical reviews have the same characteristics at a rudimentary level, as shown in Figure 4.2-5 below. The figure shows inputs, outputs, and process steps involved in performing a technical review. These characteristics are as follows:

#### 4.2.6.2.1.1 Entrance Criteria (Inputs)

Inputs to a review depend on the nature of the review and the point at which the review occurs in the development cycle. Accordingly, the primary inputs to a review consist of new products that have been generated since the previous review that reflect the advancement of the development toward completion. In addition, inputs will include products and documents that were completed in previous development phases, along with any proposed changes, to ensure that the information they contain is adequate and appropriate to proceed to the next phase. Once TPPs (or PPPs) have been established for a program, the status of these TPPs will be included as inputs to enable measurement and tracking of the maturity of the design and risks to meeting the requirements. Each review must consider the constraints under which the system is being developed, including constraints imposed by risk mitigation plans defined in previous stages.

Typical inputs to reviews include:

- Previously completed documents and products
- Service Level Mission Need
- Technical planning documents (used to define the scope, objectives, and timing of the review)
- Requirements documents and specifications, including Interface Requirements Documents (IRD) and Interface Control Documents (ICD)
- Architectures
- List of allocated TPPs and associated critical performance limits and target values
- Constraints
- Risk Mitigation Plans
- Test plans
- Proposed changes to previously completed documents and products
- Draft products and documents
- Design Analysis Reports (DAR)
- Functional analyses
- Technical Performance Measurement (TPM) reports
- Test, evaluation, verification, and validation reports

- Risk management reports

#### 4.2.6.2.1.2 Process

A prerequisite for conducting a review is the approval of the technical planning documentation that defines the objectives and scope of the review; entry criteria and items to be reviewed; the review schedule coordinated with the overall program schedule; the 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. An example of a defined approach for a Critical Design Review (CDR) is conducting design assessments on individual lower level design elements designated as Configuration Items (CI) on an incremental basis leading to a system level CDR that integrates the results of the individual lower level reviews.

The generic steps for conducting a review are:

- Define review objectives and scope
- Establish success criteria, prerequisites (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 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 and distribute review data package
- Obtain participants' responses to data package
- Assess readiness to proceed
- Collect comments to the data package (review item discrepancies)
- Update data package
- Incorporate accepted changes
- Provide summary of concerns
- Update Risk Mitigation Plans
- Conduct review
- Document the review

- Publish review minutes
- Compile action item list
- Compile issues list
- Track action items and issues
- Document closed action items and issues

#### **4.2.6.2.1.3 Exit Criteria (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 contain 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
- SLMN and gap analyses
- Requirements document(s) and specifications, including IRD/ICD
- Architectures
- Technical manuals
- Updated plans
- Risk Mitigation Plans
- Verification plans
- SEMP (TPPs)
- Approved reports
- Test reports
- TPM reports
- Risk Management Reports
- Review minutes
- Action item and issue documentation

#### 4.2.6.2.1.4 Tools

The tools used to conduct 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.

#### 4.2.6.2.1.5 Process Metrics

Metrics are preestablished criteria that measure the success of a technical review. In turn, 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:

- **Customer (stakeholder) acclimation**, which is defined as the extent of satisfaction that the review met the stated objectives. This can be measured through contract award fees, customer feedback surveys, or formal concurrence with the final review data package.
- **The number of new requirements** (system or subsystem) that surfaces at later reviews compared to the original number of requirements
- **The number of Requests For Action (RFA)** that are resolved by formal action
- **Errata** measured as the number of pages changed as a percentage of the total page count of the presentations

#### 4.2.6.2.2 Audits

Audits are used to verify the system that has been developed 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

### 4.2.6.2.3 FAA System Engineering Milestones

The FAA has established a set of reviews and audits to support its system lifecycle model (see Figure 4.2-2 above). The generic use and structure of technical reviews and audits (see subsection 4.2.6.2 above) must be tailored to some extent for each review. The tailoring details are found in Appendix C along with some best practice techniques and approaches for the following:

- Technology Readiness Assessment (TRA).** This is a multidisciplinary technical review that assesses the maturity of Critical Technology Elements (CTE) being considered to address user needs and that analyzes operational capabilities and environmental constraints within the Enterprise architectural framework. 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 enable early attention to technology maturation events. The TRA will score each identified CTE using nine Levels of Maturity (LOM) as shown in Figure 4.2-6. Technology maturity, as defined in DOD 5000.2, is “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.” (See Appendix C for details.)

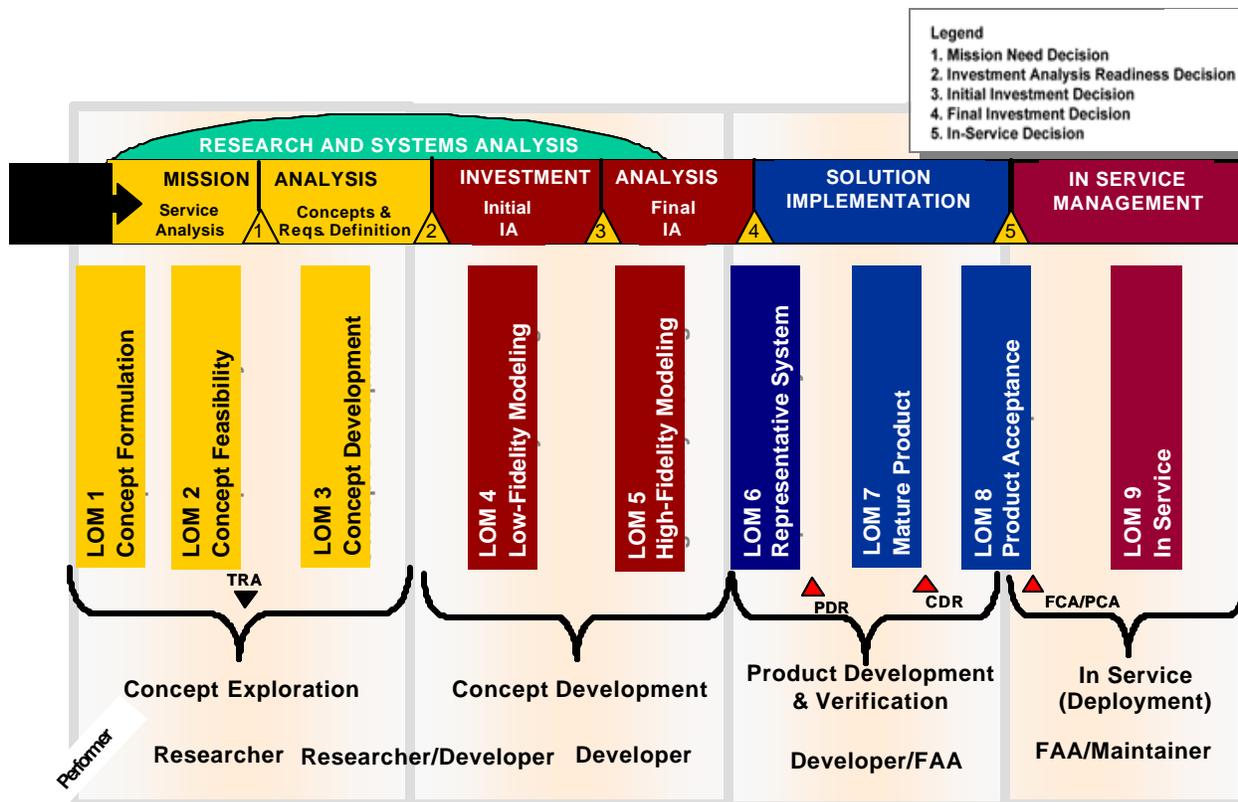


Figure 4.2-6. Technology Levels of Maturity and the System Lifecycle

- SE Investment Analysis Review (SIAR).** The SIAR determines if the mission need capabilities shortfall can be fulfilled by candidate solutions (concepts and preliminary requirements). The candidate solutions, technical constraints, and risk definition must

be sufficiently complete to support a Mission Need Decision. This checkpoint verifies that the identified needs, shortfalls, and technical constraints have been validated; that initial feasibility assessments have been accomplished; and that proposed solutions are consistent with the NAS Enterprise Architecture or required changes have been identified. The technical portion of the SIAR involves reviewing the pPR for readiness to proceed to investment analysis. The SIAR also establishes an initial set of TPPs.

- **Functional Baseline Review (FBR).** This 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 captures functional requirements that go with the Mission Analysis and Investment Analysis phases.
- **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. The SRR is generally conducted just before AMS Investment Decision (AMS Milestone 4). 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 Acquisition phase.

At the contract level, the SRR is a formal, system-level review to ensure that system requirements have been completely and properly identified and that a mutual understanding exists between the government and contractor.

- **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.
- **Verification Readiness Review (VRR).** This is a formal review of the contractors' readiness to begin verification (including testing) on both hardware and software configuration items.
- **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.
- **In Service Performance Review (ISPR).** This 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.

Each SE control gate or milestone fits within the AMS framework and supports various investment decisions as shown in Table 4.2-4. The table addresses the entry and exit criteria for both the SE milestones and AMS investment decision points to provide the reader visibility into the extent of overlap between the two needs.

Table 4.2-4. SE Milestones as a Function of AMS Lifecycle Phases (based on Nov 2005 AMS)

AMS Lifecycle Phase	SE Milestone Entry Criteria	SE Milestone	Purpose	Timing	SE Milestone Output (SE Products only)	Investment Decision Gate (AMS)
<b>Mission Analysis</b>						
<b>(Corporate)</b>	<ul style="list-style-type: none"> <li>Enterprise Architecture</li> <li>Conops</li> <li>Concerns and Issues</li> <li>Technology</li> <li>Market Research</li> <li>Need</li> <li>Corporate Strategy and Goals</li> <li>Legacy System</li> </ul>	<b>Technology Readiness Assessment Technology Readiness Assessment (TRA)</b> — a multi-disciplined technical review that assesses the maturity of Critical Technology Elements being considered to address user needs, analyzes operational capabilities and environmental constraints within the Enterprise architectural framework.	Determine extent that new and/or novel technologies may be mature enough to be considered for implementation into the NAS.		<ul style="list-style-type: none"> <li>Validated NAS Functional portion of EA</li> <li>Technology opportunities</li> <li>Updated Risk Assessment</li> <li>Gap Analysis</li> </ul>	
<b>(Service level)</b>	<ul style="list-style-type: none"> <li>Conops</li> <li>Mission Need Analysis</li> <li>Standards</li> <li>Guidance and Tools for Service level MA</li> </ul>				<ul style="list-style-type: none"> <li>Functional Architecture</li> </ul>	<b>1 - Mission Need Decision (new)</b>
<b>(Concept and Requirements Definition)</b>	<ul style="list-style-type: none"> <li>Preliminary Conuse</li> <li>FAA Policy</li> <li>Standards</li> <li>Preliminary OSED</li> <li>Constraints</li> <li>Integrated Program Schedule</li> </ul>	<b>SE Investment Analysis Review (SIAR)</b> — The intent of the SIAR is to determine if the mission need			<ul style="list-style-type: none"> <li>Service Level Mission Need (SLMN)</li> <li>Preliminary Exhibit 300 Attachment 1 (pPR — previously the iRD)</li> <li>Final</li> </ul>	<b>2 - Investment Analysis Readiness Decision (previous JRC1)</b>

AMS Lifecycle Phase	SE Milestone Entry Criteria	SE Milestone	Purpose	Timing	SE Milestone Output (SE Products only)	Investment Decision Gate (AMS)
	<ul style="list-style-type: none"> <li>Initial Description of Alternatives</li> </ul>	capabilities shortfall can be fulfilled by candidate solutions (concepts and preliminary requirements). The candidate solutions, technical constraints, and risk definition is complete enough to support a Mission Need Decision.			Description of Alternatives <ul style="list-style-type: none"> <li>Lifecycle Cost Estimate</li> <li>OSSED</li> <li>CONUSE</li> </ul>	
<b>Investment Analysis</b>						
<i>(Initial)</i>	<ul style="list-style-type: none"> <li>Preliminary Exhibit 300 Attachment 1 (pRD — previously the iRD)</li> <li>Constraints</li> <li>FAA Policy</li> <li>Standards</li> <li>IMS</li> <li>Investment risks</li> </ul>	<b>Functional Baseline Review (FBR)</b> — 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 captures functional requirements that go with the Mission Analysis and Investment Analysis phases.	It validates program cost, schedule, and performance to support Milestone approvals. It establishes the Functional baseline as the governing technical description which is required before proceeding to the next AMS phase or Decision gate.	It is generally conducted just prior to the Initial Investment Decision (AMS Investment Milestone 3).	<ul style="list-style-type: none"> <li>Final Requirements Set - Exhibit 300 Attachment 1 (previously the fRD)</li> <li>Program WBS</li> <li>Program SOW</li> <li>Final SEMP</li> </ul>	<b>3 - Initial Investment Decision (previous JRC-2A)</b>
<i>(Final)</i>	<ul style="list-style-type: none"> <li>fPR</li> <li>Architecture Impacts</li> <li>Risks</li> <li>IMS</li> </ul>	<i>(Program level)</i> <b>System Requirements Review (SRR)</b> — A	Assesses the technical readiness to begin Solution	Precedes and supports AMS Milestone	<ul style="list-style-type: none"> <li>System Specification</li> <li>Risks for recommended alternative</li> </ul>	<b>4 - Final Investment Decision (previous</b>

AMS Lifecycle Phase	SE Milestone Entry Criteria	SE Milestone	Purpose	Timing	SE Milestone Output (SE Products only)	Investment Decision Gate (AMS)
	<ul style="list-style-type: none"> <li>• LCE cost estimate of each alternative</li> <li>• Draft Interface documents</li> </ul>	formal internal FAA review ensure that the system requirements have been completely and properly identified. It is generally conducted just prior to AMS Investment Milestone 4. It validates program cost, schedule, and performance for the purpose of supporting milestone approvals. It establishes the Allocated baseline as the governing technical description which is required before proceeding to the next AMS phase.	Implementation.	4. A second SRR is conducted after AMS Milestone 4 and contract award to assess contractor's readiness to begin development.	<ul style="list-style-type: none"> <li>• LCE cost estimate for recommended alternative</li> <li>• Draft ISR Checklist</li> <li>• Interface documents</li> <li>• (Contractor) SOW</li> </ul>	<b>JRC-2B)</b>
<b>Solution Implementation</b>						
	<ul style="list-style-type: none"> <li>• System specification</li> <li>• SOW</li> <li>• Contract WBS</li> </ul>	<i>(Contract level)</i> <b>System Requirements Review (SRR)</b> — A formal, system-level review conducted to ensure that system requirements have been completely and properly identified and that a mutual understanding	Assesses the Contractor's readiness to begin development	After contract award and prior to functional allocation activities begin	<ul style="list-style-type: none"> <li>• Agreement on system specification</li> </ul>	

AMS Lifecycle Phase	SE Milestone Entry Criteria	SE Milestone	Purpose	Timing	SE Milestone Output (SE Products only)	Investment Decision Gate (AMS)
		between the government and contractor exists.				
<b><i>(Preliminary design)</i></b>	<ul style="list-style-type: none"> <li>Completed allocated baseline as documented in design specifications for each hardware and software configuration item.</li> </ul>	<b>Preliminary Design Review (PDR)</b> — A formal review that confirms the preliminary design logically follows the SFR findings and meets requirements. It normally results in approval to begin detailed design.	Assesses the preliminary design against the Allocated baseline and readiness to begin detailed design.	At completion of functional allocation activities and prior to beginning detailed design	<ul style="list-style-type: none"> <li>(Approval to begin detail design)</li> <li>Risks</li> <li>RFA</li> </ul>	
<b><i>(Detail design)</i></b>	<ul style="list-style-type: none"> <li>Completed design package for each hardware and software configuration item.</li> </ul>	<b>Critical Design Review (CDR)</b> — A formal review conducted to evaluate the completeness of the design, its interfaces, and suitability to start initial manufacturing.	Assesses the preliminary system product design package against the Allocated baseline.	At completion of CI detail design activities and prior to fabrication of hardware and coding of final software modules (the "90%" design point)	<ul style="list-style-type: none"> <li>(Approval to begin fabrication)</li> <li>Risks</li> <li>RFA</li> </ul>	
<b><i>(Verification)</i></b>	<ul style="list-style-type: none"> <li>System definition is under formal configuration control</li> <li>All verification plans approved</li> <li>Draft verification procedures</li> </ul>	<b>Verification Readiness Review (VRR)</b> — A formal review of contractors' readiness to begin verification (including testing) on both hardware and	Assesses the readiness to begin product technical evaluation.	At completion of system fabrication and prior to initiation of formal verification activities	<ul style="list-style-type: none"> <li>(Approval to begin formal verification)</li> <li>Risks</li> <li>Detailed verification procedures</li> </ul>	

AMS Lifecycle Phase	SE Milestone Entry Criteria	SE Milestone	Purpose	Timing	SE Milestone Output (SE Products only)	Investment Decision Gate (AMS)
	available <ul style="list-style-type: none"> <li>• Verification assets/resources identified and available.</li> </ul>	software configuration items.				
	<ul style="list-style-type: none"> <li>• Verification program complete</li> <li>• Reports approved</li> <li>• Verification article configuration compliance to design package established</li> </ul>	<b>Functional Configuration Audit (FCA)</b> — 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.	Assesses the as-built system's functional compliance with the product baseline & supports completion of PCA.	At completion of qualification and integration testing and prior to delivery of first production article.	<ul style="list-style-type: none"> <li>• Configuration reconciliation list</li> <li>• Gap of required versus verified performance</li> </ul>	
	<ul style="list-style-type: none"> <li>• Technical data package complete</li> <li>• Quality control results available</li> <li>• Manufacturing and quality control plans complete</li> <li>• FCA complete</li> <li>• Configuration differences between FCA and PCA units reconciled</li> </ul>	<b>Physical Configuration Audit (PCA)</b> —A formal audit that establishes the product baseline as reflected in an early production configuration item.	Assesses the as-delivered system's compliance with the product baseline.  Supports the AMS Milestone 5 (In Service Decision).  Establishes CM control transfer from Implementor to Owner.	After delivery of initial production unit and prior to CAI	<ul style="list-style-type: none"> <li>• Baselined hardware/software configuration</li> <li>• Operator and user manuals</li> </ul>	<b>5 - In-Service Decision (same)</b>
<b>In-Service Management</b>						
		<b>In Service Performance Review (ISPR)</b> — A				

AMS Lifecycle Phase	SE Milestone Entry Criteria	SE Milestone	Purpose	Timing	SE Milestone Output (SE Products only)	Investment Decision Gate (AMS)
		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.				

#### 4.2.7 Integrated Technical Planning Metrics

The primary integrated planning metric is publication and approval of the SEMP, supporting technical plans, and the ISAP at each AMS milestone.

#### 4.2.8 Integrated Technical Planning Tools

Integrated Technical Planning 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.

#### 4.2.9 References

1. Kevin Forsberg, Hal Mooz, and Howard Cotterman. *Visualizing Project Management: Models and Frameworks for Mastering Complex Systems*. 3rd edition (hardcover). New York, NY: John Wiley & Sons, September 1, 2005.
2. *Practice Standard for Work Breakdown Structures*. Project Management Institute, Inc., Four Campus Boulevard, Newtown Square, PA, 10973, 2001.
3. Pritchard, Carl. *How to Build a Work Breakdown Structure*. The Cornerstone of Project Management. ESI International, 4301 Fairfax Drive, Arlington, VA 22203, 1998.

## 4.3 Requirements Management

### 4.3.1 Introduction to Requirements Management

The Requirements Management process, an element of System Engineering (SE), **is an activity that spans the program's entire lifecycle. Requirements Management iteratively identifies and refines the top-level requirements to successively lower levels, in concert with functional baselines and architectures, and synthesis of solutions established for the system of interest.** For the purposes of Requirements Management, a system or a product means any physical product or software being designed, developed, and/or produced, or any intangible product, such as a product describing a process or a service.

#### 4.3.1.1 Requirements Definitions

##### 4.3.1.1.1 Requirement

A requirement is ***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.***

##### 4.3.1.1.2 Requirement Set

A Requirement Set is ***an aggregate of requirements for a system that specifies its characteristics in totality.***

##### 4.3.1.1.3 Requirements Analysis

Requirements Analysis is ***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.***

##### 4.3.1.1.4 Requirements Management

Requirements Management is ***a process performed throughout a system's life to elicit, identify, develop, manage, and control requirements and associated documentation in a consistent, traceable, correlatable, verifiable manner.*** It ensures solution compliance with stakeholder needs and expectations using allocation, verification, and adaptation to and control of changes.

#### 4.3.1.2 Process Description

##### 4.3.1.2.1 Purpose

Requirements Management establishes a layered approach that defines the essential system characteristics and all system components required for the product's successful development, production, deployment, operation, and disposal. Successful completion of this process is measured by the acceptable transformation of stakeholder needs into discrete, verifiable, low-level requirements. The process identifies, clarifies, balances, and manages the entire requirements set through interactive dialogue with all stakeholders. Figure 4.3-1 shows the top-level process.

The Requirements Management process defines, collects, documents, and manages all requirements, including the complete requirements set consisting of the Service Level Mission Need (SLMN), the preliminary Program Requirements (pPR) and final Program Requirements (fPR), and the system and procurement specifications.

Executing this process results in an authorized, organized, and baselined set of requirements for a product. These requirements are presented as requirements sets, usually as requirements documents, to all other applicable SE and Federal Aviation Administration (FAA) processes. To effectively develop and manage system requirements, one must develop all requirements through this process.

#### **4.3.1.2.2 Requirements Management Objectives**

Requirements Management is an iterative process that:

- Identifies and captures the requirements applicable to the system
- Analyzes and decomposes the requirements into clear, unambiguous, traceable, and verifiable requirements
- Derives lower level requirements from higher level requirements in the system hierarchy
- Allocates the requirements to the appropriate component within the system hierarchy and/or to the appropriate organizational entities
- Establishes the method of verification for each requirement
- Ensures that the product complies with the requirements
- Manages, documents, and controls the requirements and changes to them in a traceable manner

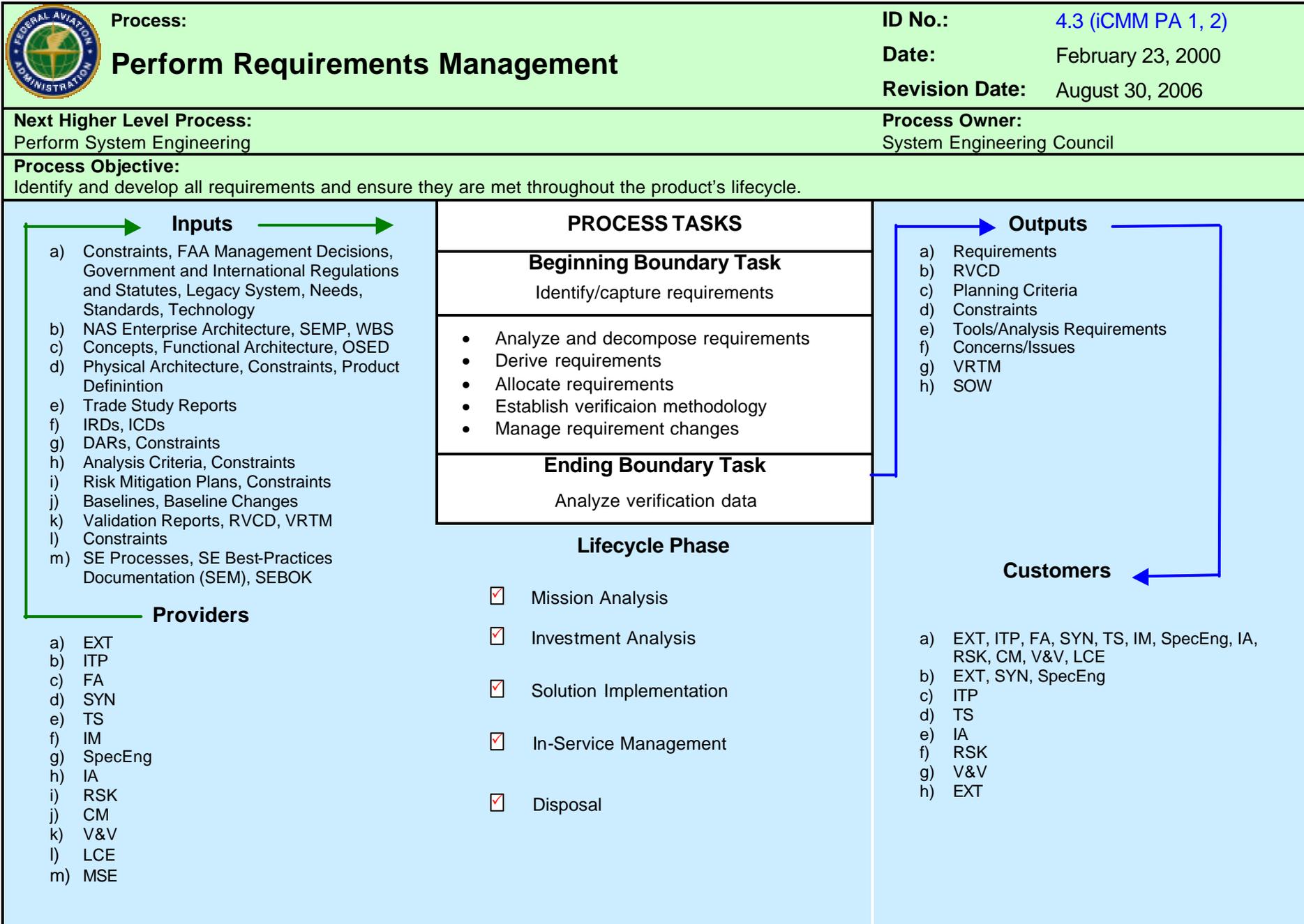


Figure 4.3-1. Requirements Management Process-Based Management Chart

### 4.3.1.3 Management

The Requirements Management process bridges integrated product development system stages. The products are baselined in accordance with the milestones established in the Integrated Program Plan for the applicable project. Prerequisites for successful performance of the process are:

- Empowering a requirements analysis team with the authority and mission to execute the process
- Assigning an experienced team leader knowledgeable in SE principles and committed to the standard SE methods documented herein
- Assigning team members that are experienced and knowledgeable in relevant engineering, manufacturing, operational, specialty engineering, and support disciplines
- Establishing the criteria for decision making and any supporting tools
- Completing relevant training of team members in using this process and relevant tools
- Defining the formats of the output deliverables from this activity

### 4.3.1.4 Requirements Management Process Flow

Requirements Management is an iterative process that works with Functional Analysis and Synthesis to produce requirements. The process begins with the identified need and repeats through successively more detailed layers until requirements are detailed enough for their intended purpose. Figure 4.3-2 illustrates the FAA Requirements Management process flow that starts with the National Airspace System (NAS) Concept of Operations (CONOPS) and ends with the System Specification that will be used for system acquisition.

Starting from the NAS and NAS Enterprise Architecture, the initial Functional Analysis produces the System CONOPS. The functions described in the System CONOPS are the first inputs to the Identify and Capture requirements step of the Requirements Management process. These functions, along with the performance and nonfunctional requirements, are formed into the first system requirements and documented in the SLMN. At this point in the process, there is insufficient detail in the requirements to synthesize a physical architecture, so the synthesis step is not performed.

After the SLMN is completed during the first pass through the requirements process, the System CONOPS is further decomposed using the Functional Analysis process, as constrained by the requirements defined in the SLMN. This level of functional analysis produces the first level of the functional architecture and is used to refine the SLMN-level requirements into the initial requirements that are documented in the pPR. The pPRs are used to define the first version of the physical architecture during the Synthesis process.

The process then repeats to produce the fPR. The functional architecture, which is constrained by the pPR requirements, is decomposed. The fPRs are then decomposed from the functional architecture, which is constrained by the pPR-level physical architecture. The pPR-level physical architecture, which is refined by the fPR requirements, is used to derive the physical architecture at the fPR level.

The process then repeats a final time to produce the System Level Specification. The functional architecture, which is constrained by the fPRs, is decomposed. The System Specification requirements are then developed from the functional architecture, which is constrained by the fPR-level physical architecture. The fPR-level physical architecture, which is refined by the System Specification requirements, is used to derive the physical architecture at the System Specification level.

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 through the process until the lower levels reflect the changes.

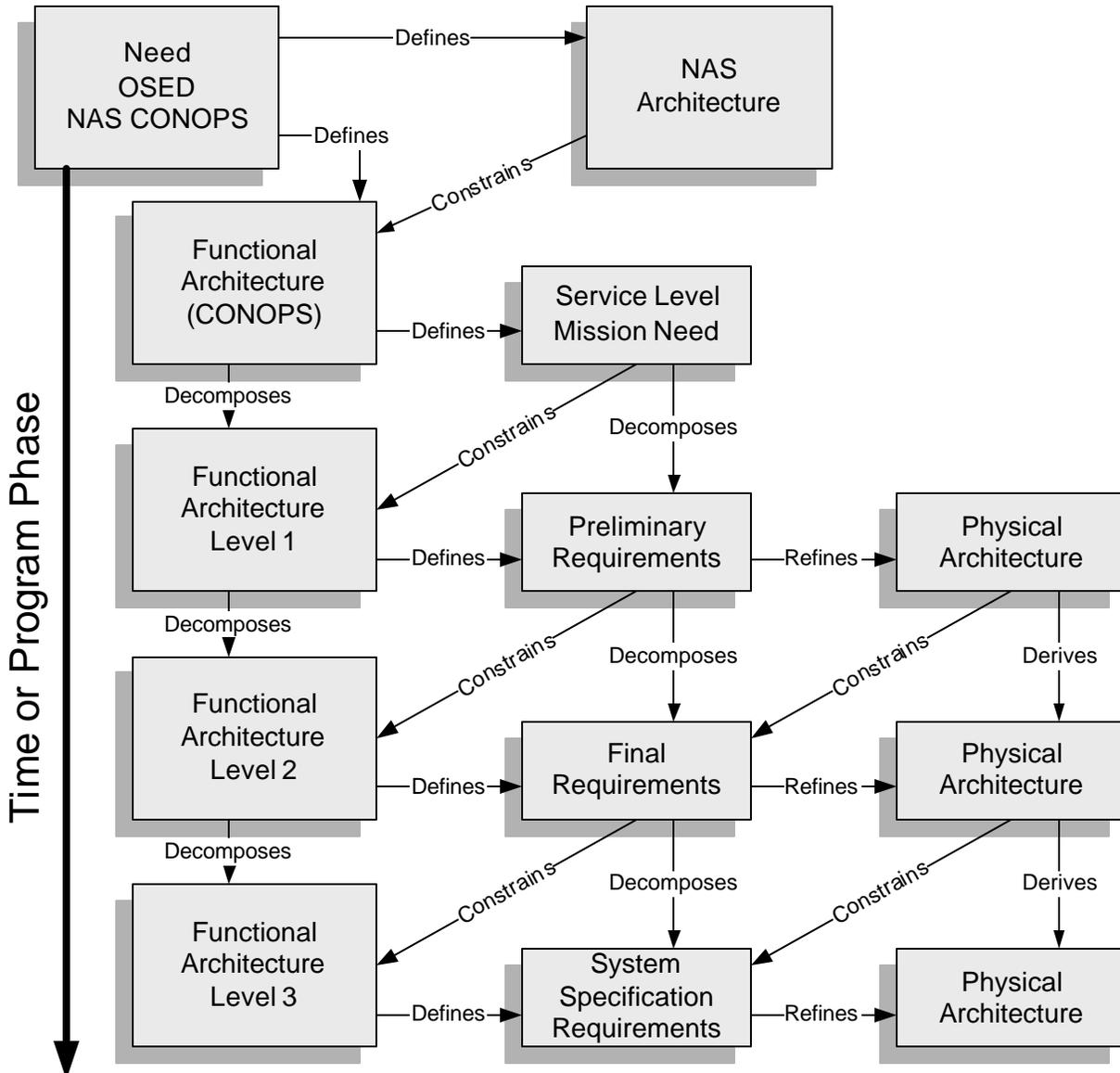


Figure 4.3-2. Requirements Management Process Flow

## 4.3.2 Inputs to Requirements Management

An input to the Requirements Management process **is information received during the process**. Inputs are classified according to their source, shown in Figure 4.3-3 to be either external or internal. External inputs come from sources outside SE. Internal inputs come from the other SE processes described in this manual.

Input requirements are comprehensive and defined for both system products and system processes, including the eight lifecycle functions of development, manufacturing, verification, deployment, operations, support, training, and disposal. Requirements Management is an iterative process that flows from a high level to a low level of requirements (as shown in Figure 4.3-2 above). Therefore, some of the inputs described in the following subsections may be inputs to one stage of the requirements development process and outputs of other stages.

All requirements sources described are inputs at one point in the process and are captured. The inputs to the Requirements Management process are described in the following subsections.

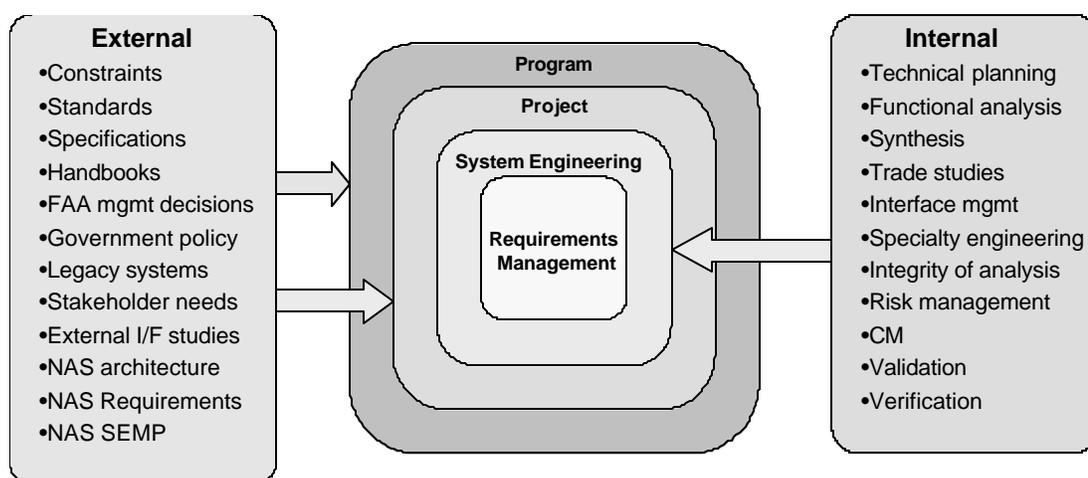


Figure 4.3-3. Input Sources to Requirements Management

### 4.3.2.1 External Inputs

External inputs come to the Requirements Management process from outside SE's boundaries.

#### 4.3.2.1.1 Constraints

A Constraint is ***an internal or externally imposed boundary condition that places limits within which the system or process must remain.***

##### 4.3.2.1.1.1 External Constraints

External constraints, including guidelines and assumptions, are identified. External constraints are imposed from outside the project or system boundaries. External conditions under which the mission is to be performed and systems developed are described. The conditions may

include performance, technology, use of infrastructure, and labor/management agreement constraints. Additional assumptions concerning programmatic, technology, and environments that may be required are captured.

#### 4.3.2.1.1.2 Internal Constraints

Internal constraints—including assumptions, guidelines, and program-specific constraints—are identified. Internal constraints are imposed from within the project or system boundaries but outside of the SE process boundary. Program-specific conditions under which the mission is to be performed and systems developed are described. The conditions may include performance, technology, and use of infrastructure constraints. Additional assumptions concerning programmatic, technology, and environments that may be required are captured.

#### 4.3.2.1.2 Standards, Specifications, and Handbooks

Specified government standards, external standards, and general specifications or handbooks to be used on the program are identified. The most common standards, specifications, and handbooks used in FAA requirements management appear in Appendix G.

##### 4.3.2.1.2.1 Standards

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 for material. The FAA, Department of Defense (DoD), and other U.S. Government agencies, as well as the RTCA, international organizations, and commercial standards organizations publish standards.

##### 4.3.2.1.2.1.1 RTCA Standards

The RTCA publishes standards as Minimum Operational Performance Standards (MOPS) and Minimum Aviation System Performance Standards (MASPS).

##### 4.3.2.1.2.1.1.1 Minimum Operational Performance Standards

The MOPS contain performance requirements for avionics. The standards describe typical equipment applications and operational goals and establish 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.

##### 4.3.2.1.2.1.1.2 Minimum Aviation System Performance Standards

The MASPS address the user-level service requirements used to qualify the 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.

#### 4.3.2.1.2.2 Specifications

A specification is ***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.*** The FAA, DoD, and other U.S. Government agencies; international organizations; and commercial standards organizations publish specifications.

#### 4.3.2.1.2.3 Handbooks

A handbook is ***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. Handbooks provide industry with reference materials that help to standardize FAA assets. Use of handbooks is optional unless required by a specification or contract document. The FAA, DoD, and other U.S. Government agencies; international organizations; and commercial standards organizations publish handbooks.

#### 4.3.2.1.2.4 Federal Aviation Administration Orders

An FAA order is ***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 cannot obligate contractors. Thus, orders are not used in contract documents. They are not referenced in requirements documents but are used as inputs with the potential to generate requirements.

#### 4.3.2.1.2.5 National Airspace System Master Configuration Index

NAS-MD-001, "National Airspace System Master Configuration Index," lists all baselined systems, equipment, and software currently operational or under procurement for the National Airspace System (NAS) with current approved baseline documentation. FAA and contractor personnel use NAS-MD-001 to identify configuration items and documentation requiring NAS Change Proposals (NCP).

#### 4.3.2.1.3 Federal Aviation Administration Management Decisions

Management decisions that are imposed on the system from the national, department, or agency level are captured.

#### 4.3.2.1.4 Government Policy

##### 4.3.2.1.4.1 Government Regulations and Statutes

Government statutes and military and civilian regulations impacting the system are identified, including requirements incorporated into Executive orders and legislation (e.g., safety or security requirements). These requirements also include government standards that have been mandated as part of a contract.

#### **4.3.2.1.4.2 International Policy**

The International Civil Aviation Organization (ICAO) develops and publishes international Standards and Recommended Practices (SARP). An ICAO standard is any specification for physical characteristics, configuration, material performance, personnel, or procedure that is applied uniformly for the safety or regulation of international air navigation and to which the international aviation community conforms. An ICAO-recommended practice is identical to a standard except that it is not considered necessary—only desirable.

#### **4.3.2.1.4.3 Federal Aviation Administration Policy**

This category covers all FAA agencywide management decisions and policy requirements imposed by FAA agencywide mandate. The category may include technical, operational, acquisition, financial, and other requirements. FAA policy is invoked using the FAA Directives System, as described in FAA Order 1320.1, “FAA Directives System.”

#### **4.3.2.1.4.4 Acquisition Management System**

New or revised directions and limitations established by the Acquisition Management System (AMS) are identified.

#### **4.3.2.1.5 Legacy Systems**

Requirements from past and current systems are captured and analyzed for applicability. Data for legacy systems are in FAA specifications and technical instruction books.

#### **4.3.2.1.6 Stakeholder Needs**

##### **4.3.2.1.6.1 National Airspace System Concepts of Operations Document**

The NAS Concepts of Operations (CONOPS) document provides a CONOPS from the perspectives of NAS users and service providers. It is the basis for an incremental benefits-driven approach toward NAS evolution. The document is arranged in a phases-of-flight approach, including Flight Planning, Surface, Arrival/Departure, En Route, and NAS Management. It is the source document for all NAS operational requirements.

##### **4.3.2.1.6.2 Service Level Mission Need**

The SLMN is the first document to translate the NAS 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. The SLMN justifies, in rigorous analytical terms, the need to resolve a shortfall in services required by its users and service providers or to explore a technological opportunity for more efficient and effective mission performance. The SLMN identifies the mission area, needed capability, current capability, capability shortfall, impact to users and service providers if the shortfall is not resolved, benefits, timeframe for resolving the shortfall, criticality of the mission, and resource estimate.

#### 4.3.2.1.6.3 Operational Scenarios

Operational scenarios provided by the user describe how the CONOPS is implemented. The scenarios may include interactions with the environment and other systems, human tasks and task sequences, and physical interconnections with interfacing systems or products. They may be incorporated into the SLMN or provided as a separate document.

#### 4.3.2.1.6.4 Requirements Document

A Requirements Document is *a collection of requirements and related information or attributes presented in a user-defined format.*

The document establishes the operational framework and performance baseline and traces Functional Analysis to the NAS CONOPS and the SLMN; it also is the primary source document for the system-level requirements. This document is the principal force driving the search for a realistic and affordable solution to the mission need. The pPR document is developed early in the process by the sponsoring organization. It primarily provides a set of requirements that are used to evaluate the chosen alternatives. The document translates the need in the SLMN into initial top-level requirements that address such concerns as performance, supportability, physical and functional integration, human integration, security, test and evaluation, implementation and transition, quality assurance, configuration management, and in-service management. The pPR document does not describe a specific solution to a mission need. It is recommended that the document not preclude leasing, commercial, or nondevelopment solutions. The fPR document defines exactly the operational concept and requirements that are to be achieved and is the basis for evaluating the readiness of resultant products and services to become operational. The fPR document details the functional and performance requirements of the chosen alternatives and, when baselined, constitutes the functional baseline. The fPR document is the basis for developing the system-level specification.

The various requirements documents are developed in an iterative process that starts with the basic CONOPS and progresses through the SLMN, pPR, fPR, and eventually to the system level specification. Due to this iterative nature of the Requirements Management process, any of the requirements documents can be *both an input to and an output of the process.*

#### 4.3.2.1.7 External Interface Studies

System external interface studies and analyses that characterize and define the interfaces between the system and external environment are reviewed or conducted. These studies identify functional and physical characteristics between two or more elements that are provided by different agencies; they also resolve problems. Topics include issues, option assessments, impact assessments, interfaces and connections, sources of interferences, and configuration options.

#### 4.3.2.1.8 National Airspace System Requirements

##### 4.3.2.1.8.1 NAS Systems Requirements Specification (NAS-SR-1000)

This FAA document defines the NAS Level operational requirements and is the approved baseline document for operational requirements for the NAS. The document serves as a basis to perform studies and analysis and to identify engineering concepts to satisfy operational requirements. It also serves as a source document for system level specification preparation.

#### **4.3.2.1.8.2 NAS Design Specification (NAS-DD-1000)**

This baselined FAA document defines the NAS Level functional architecture, including basic NAS elements, sub-elements, subsystems, and their interrelationships.

#### **4.3.2.1.8.3 NAS System Specification (NAS-SS-1000)**

This baselined FAA document defines functional, performance, design, construction, logistics, personnel and training, documentation, verification, and interface requirements for the NAS.

### **4.3.2.2 Internal Inputs**

Internal inputs come to the Requirements Management process from inside SE's boundaries and include inputs for all other SE processes (as shown in Figure 4.3-3 above). Execution of the other SE processes may generate constraints that impact the Requirements Management process. These constraints are identified and provided as inputs to the Requirements Management process and may result in derived requirements in step 3 (subsection 4.3.3.3 below) of the process.

#### **4.3.2.2.1 Integrated Technical Planning**

The Requirements Management planning section of the Implementation Strategy and Planning document (ISAP) and the System Engineering Management Plan (SEMP) (see Integrated Technical Planning (Section 4.2)) specify the tasks, products, responsibilities, and schedules for managing requirements throughout product development. It details the total effort for managing requirements. This work includes "Step 1: Identify and Capture Requirements" (subsection 4.3.3.1 below); "Step 2: Analyze and Decompose Requirements" (subsection 4.3.3.2); "Step 3: Derive Requirements" (subsection 4.3.3.3); "Step 4: Allocate Requirements" (subsection 4.3.3.4); and "Step 6: Manage Requirements Changes" (subsection 4.3.3.6).

##### **4.3.2.2.1.1 NAS Enterprise Architecture**

The NAS Enterprise Architecture is a strategic and evolutionary plan for modernizing the NAS that supports investment analysis tradeoffs. It defines and delivers the services that meet aviation industry and public needs 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 that 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. The NAS Enterprise Architecture presents a comprehensive design that shows each major mechanism within the NAS, including interfaces and data flows. Using a documented design with traceable requirements as the foundation for the architecture not only provides a complete picture of the NAS, but it also provides a roadmap for implementing future enhancements.

##### **4.3.2.2.1.2 System Engineering Management Plan**

The SEMP relates the technical requirements to program requirements, providing the structure to guide and control requirements management activities to achieve the SE objectives consistent with a top-level management plan for the program.

#### 4.3.2.2.1.3 Work Breakdown Structure (WBS)

The WBS provides a logical structure for developing the requirements.

#### 4.3.2.2.2 Functional Analysis

##### 4.3.2.2.2.1 Concept of Operations

A CONOPS is *a description of what is expected from the system, including its various modes of operation and time-critical parameters*. The CONOPS is obtained from the Functional Analysis process (Section 4.4). The CONOPS document communicates overall quantitative and qualitative system characteristics to the user, buyer, developer, and other organizational elements. The CONOPS aids in requirements capture and communicates the need to the developing organization. The CONOPS describes the existing system, current environment, users, interactions among users and the system, and organizational impacts. A CONOPS is essentially a top-level narrative Functional Analysis and is the basis for developing the SLMN.

##### 4.3.2.2.2.2 Functional Architecture

Every function required to satisfy a system's operational needs is identified and defined. Once defined, the functions are used to define system requirements, and a functional architecture is developed based on the identified requirements. The process is then taken to a greater level of detail, as the identified functions are further decomposed into subfunctions, and the functional architecture and requirements associated with those functions are each decomposed as well. This process is iterated until the system has been completely decomposed into basic subfunctions, and each subfunction at the lowest level is completely, simply, and uniquely defined by its requirements. In this process, the interfaces between each of the functions and subfunctions are fully defined, as are the interfaces within the environment and external systems. The functions and subfunctions are arrayed in a functional architecture to show their relationships and internal and external interfaces.

The functional architecture includes a definition of the functions that the system needs to perform and is developed into Primitive Requirements Statements (PRS). "Step 2: Analyze and Decompose Requirements" (subsection 4.3.3.2 below) of the Requirements Management process develops these PRSs into Mature Requirements Statements (MRS).

##### 4.3.2.2.2.3 Operational Services and Environmental Description

The Operational Services and Environmental Description (OSED) is a comprehensive, holistic description of the services, environment, functions, and mechanizations that form a system's characteristics. It consists of everything inside and outside the system that affects system performance and that is affected by system operation or both. Functional Analysis (Section 4.4) fully describes the OSED.

The OSED is used as a source to derive lower level requirements. It describes many system characteristics that are nonfunctional, such as environments, and that are not described in the functional architecture. Nonfunctional requirements are derived from the OSED in "Step 3: Derive Requirements" (subsection 4.3.3.3 below).

### **4.3.2.2.3 Synthesis**

#### **4.3.2.2.3.1 Physical Architecture**

The physical architecture allocates requirements to the physical hardware and/or software during the Synthesis process (Section 4.5). If requirements conflicts are discovered during the development of the physical architecture, those requirements are cycled back through the Requirements Management process for evaluation, which may result in conducting a trade study (see Section 4.6), reallocating the requirement, or deriving lower-level requirements. The RAM describes requirements allocation.

#### **4.3.2.2.3.2 Constraints**

Constraints that are discovered during synthesis—including cost, schedule, programmatic, technology, and so forth—that will have an impact on requirements are returned to Requirements Management for input into the requirements process. The constraints identified in synthesis may introduce derived requirements. These derived requirements (Step 3: Derive Requirements (subsection 4.3.3.3)) may be developed through Synthesis (Section 4.5) and are generally not provided by external sources, such as the user, service provider, or government agencies.

#### **4.3.2.2.4 Trade Studies**

Trade Studies (Section 4.6) may be conducted within and across functions to support decisions during any stage of the system's lifecycle. They quantify through metrics the consequences of opting for various system alternatives, traceable to stakeholder requirements that may be imposed by the requirements development process. They support allocating performance requirements and determining requirements or Design Constraints; they are also used in evaluating alternatives. Trade Studies usually result in derived requirements that are developed into MRSs in "Step 2: Analyze and Decompose Requirements" (subsection 4.3.3.2).

##### **4.3.2.2.4.1 Trade Study Reports**

Trade Study Reports identify requirements that are affected by the results of each trade study (see Section 4.6). The new, changed, or derived requirements flow through the entire Requirements Management process and may result in changes to the requirements baseline. Trade Study Reports document the results of feasibility assessments and communicate derived requirements to the Requirements Management activity.

###### **4.3.2.2.4.1.1 Feasibility Assessments**

The Feasibility Assessment may be conducted to assess the difficulty in achieving program goals within the Constraints. Assessment results consider various aspects, such as technical, cost, and schedule, across the lifecycle. It provides information on the expectations for success, considering identified technology development needs in view of program and mission schedule and cost constraints. It also assesses the range of costs and benefits associated with several alternatives for solving a problem.

#### **4.3.2.2.4.1.2 Derived Requirements**

Derived requirements (“Step 3: Derive Requirements” (subsection 4.3.3.3)) may be developed through Trade Studies (Section 4.6) and not provided by external sources, such as the user, service provider, or government agencies. Derived requirements are returned to Requirements Management for analysis and possible inclusion in the requirements baseline.

#### **4.3.2.2.5 Interface Management**

The inputs from Interface Management (Section 4.7) identify, describe, and define interface requirements to ensure compatibility between interrelated systems and between system elements.

##### **4.3.2.2.5.1 Interface Requirements Document**

The Interface Requirements Document (IRD) defines requirements associated with external physical and functional interfaces between the particular system and other associated system(s).

##### **4.3.2.2.5.2 Interface Control Document**

The Interface Control Document (ICD) is a design document that describes the detailed, as-built implementation of the functional requirements in the IRD.

#### **4.3.2.2.6 Specialty Engineering**

Specialty Engineering (Section 4.8) 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. Specialty Engineering studies often find characteristics that create a need for new or different requirements or a conflict between two or more requirements. The Specialty Engineering process develops the new or changed requirements, which become inputs to the Requirements Management process through the Design Analysis Report.

##### **4.3.2.2.6.1 Design Analysis Reports**

Design Analysis Reports (DAR), which document the results of a specific Specialty Engineering analysis with rationale, are inputs to the Requirements Management process. Each DAR contains a description of the system's special characteristics, a list of existing requirements that have undergone the Validation and Verification process (Section 4.12), residual risks, and candidate requirements derived from Specialty Engineering analysis.

The rationale supplementing the DARs includes the scope, ground rules, assumptions, constraints, methods, and tools applicable to the analysis.

##### **4.3.2.2.6.2 Constraints**

Constraints that are discovered conducting specialty engineering analysis—including cost, schedule, programmatic, technology, and so forth—that will have an impact on requirements are returned to Requirements Management for input into the requirements process. The constraints identified in Specialty Engineering may introduce derived requirements. These derived requirements (Step 3: Derive Requirements (subsection 4.3.3.3)) may be developed through

Specialty Engineering and are generally not provided by external sources, such as the user, service provider, or government agencies

#### **4.3.2.2.7 Integrity of Analysis**

##### **4.3.2.2.7.1 Analysis Criteria**

If the Requirements Management process requires an analysis or selection of a tool, Analysis Criteria for that analysis or selection are captured. The Analysis Criteria for conducting a required analysis is in the Analysis Management Plan (AMP).

##### **4.3.2.2.7.2 Constraints**

Any constraints driven by tool selection, skill requirements, or other programmatic considerations documented in the AMP are furnished to the Requirements.

#### **4.3.2.2.8 Risk Management**

##### **4.3.2.2.8.1 Risk Mitigation Plans**

The Risk Management (Section 4.10) process analyzes Concerns and Issues that any SE process identifies. Risk Mitigation Plans that result from risk analysis become inputs to the Requirements Management process. Requirements that present a risk are processed through the Requirements Management process for reanalysis, rederivation, and reallocation as needed.

##### **4.3.2.2.8.2 Constraints**

Constraints that are discovered in conducting risk management activities—including cost, schedule, programmatic, technology, and so forth—that will have an impact on requirements are returned to Requirements Management for input into the requirements process. The constraints identified in Risk Management may introduce derived requirements. These derived requirements may be developed through Step 3: Derive Requirements (subsection 4.3.3.3).

#### **4.3.2.2.9 Configuration Management**

##### **4.3.2.2.9.1 Baselines**

The Configuration Management process (Section 4.11) establishes baselines. After the responsible authority approves the baselines, Requirements Management updates and maintains the baseline requirements set.

##### **4.3.2.2.9.2 Baseline Changes**

Changes to the baselined requirements set are captured from the Configuration Management process (Section 4.11). “Step 6: Manage Requirements Changes” (subsection 4.3.3.6) inserts the baseline changes into the requirements set.

#### 4.3.2.2.9.3 Configuration Status Accounting Reports

Configuration Status Accounting Reports are captured from the Configuration Management process (Section 4.11). “Step 6: Manage Requirements Changes” (subsection 4.3.3.6) uses these reports to maintain a status accounting of all requirements.

#### 4.3.2.2.10 Validation

The Validation process (Section 4.12) determines if the requirements produced by the Requirements Management process are sufficiently correct and complete. Requirements that are not validated are captured and resubmitted to the Requirements Management process.

##### 4.3.2.2.10.1 Validation Report

The Validation Report summarizes the results of the Validation process (Section 4.12) and communicates the Validation Table to the Requirements Management process.

The Validation Report contains:

- Summary of validation results
- Description of the system and program
- Validation methodology used
- Unvalidated requirements
  - List of nonconforming requirements
  - Recommendations for correction of nonconforming requirements
- Validation Table
- Discussion of trends and patterns of failure, evidence of systemic failings, and emerging threats to system services

##### 4.3.2.2.10.1.1 Validation Table

The Validation Table lists all requirements and describes:

- If a requirement has been validated
- Where the requirement may be found
- Source of validation
- Corrective action to be taken if necessary
- Corrective action owner

Table 4.12-1 in Validation and Verification (Section 4.12) is an example of a Validation Table. The completed table is in the requirements document and is the basis for the Verification process.

#### **4.3.2.2.11 Verification**

The Verification process (Section 4.12) determines that the design solution satisfies applicable requirements.

##### **4.3.2.2.11.1 Verification Requirements Traceability Matrix**

The Verification Requirements Traceability Matrix (VRTM) is the heart of the Verification process. A Verification Requirement specifies the strategy or method used to verify each requirement, and the VRTM lists the Verification Requirements. 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. The VRTM establishes the basis for the verification program. The Requirements Management process initiates the VRTM and sends it to the Verification process, which returns the VRTM to Requirements Management when verification has been completed.

##### **4.3.2.2.11.2 Requirements Verification Compliance Document**

The Requirements Verification Compliance Document (RVCD) provides 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 verification methods and corresponding compliance information. The results of the Verification process (Section 4.12), 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, as well as a description and disposition of conformance, nonconformance, conclusions, and recommendations. 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 noncompliance. It is recommended that this section also specify appropriate reverification procedures. The Requirements Management process captures noncompliant requirements, leading to a decision on disposition of these requirements.

#### **4.3.2.2.12 Lifecycle Engineering**

##### **4.3.2.2.12.1 Constraints**

Constraints provided by Lifecycle Engineering to Requirements Management elements are Earned Value Management variances associated for each phase of the system lifecycle. These metrics are used to report cost, schedule, and technical performance associated with each service level. The constraints identified in Lifecycle Engineering may introduce derived requirements. These derived requirements may be developed through Step 3: Derive Requirements (subsection 4.3.3.3).

### **4.3.3 Requirements Management Process Steps**

The following steps are necessary to perform Requirements Management:

- Identify and Capture Requirements
- Analyze and Decompose Requirements
- Derive Requirements

- Allocate Requirements
- Establish Requirements Verification Methods
- Manage Requirements

### 4.3.3.1 Step 1: Identify and Capture Requirements

#### 4.3.3.1.1 Introduction

This step identifies, prioritizes, and extracts all written directives, including documented stakeholder negotiations/discussions, and internally derived requirements that are relevant to the particular stage of the system lifecycle.

This activity is performed on the entire system, including any requirements that are known at this stage about how the system will perform during its lifecycle and any constraints imposed on the system design/production by stakeholders and internal functions (i.e., manufacturing, product support, agency-level policies, suppliers).

#### 4.3.3.1.2 Scope

The scope of the requirements set includes sufficient specification of all the system functions and all the external interfacing systems, including the system environment. This step may require considering a wider domain than the immediate physical boundary of the product and its components. Different boundaries may need to be defined for different states, modes, and capabilities. Refinement of these boundary definitions is an iterative process that occurs as more information is discovered about the true nature of the required system functions and performance.

#### 4.3.3.1.3 Detailed Step 1 Description

Figure 4.3-4 describes the flow of the Identify and Capture Requirements step.

##### 4.3.3.1.3.1 Step 1.1: Define Stakeholder Needs

Stakeholder needs are defined and quantified, and stakeholder needs in the FAA come from the operational stakeholder in the form of:

- CONOPS
- SLMN
- pPR or fPR

They are transformed into baselined requirements sets at a successively lower level through iteration of the Requirements Management 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 as well as on human engineering; knowledge, skills, and abilities; availability; reliability; safety; and training requirements of the humans required to support lifecycle processes. 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., funding, cost or price objectives, schedule, technology, non-developmental and reusable items, physical characteristics, and hours of operation per day)

#### **4.3.3.1.3.2 Step 1.2: Define Project and Corporate Constraints**

Project and corporate constraints that impact design solutions are identified and defined. The NAS Enterprise Architecture may also impose long-range planning constraints through the approved capabilities and operational improvements.

##### **4.3.3.1.3.2.1 Project Constraints**

Project constraints include:

- Existing approved specifications and baselines
- Updated NAS Enterprise Architecture operational improvements
- Updated NAS Enterprise Architecture segments and mechanisms
- 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

##### **4.3.3.1.3.2.2 Corporate Constraints**

Corporate constraints include:

- Management decisions from the Joint Resources Council or other management review
- FAA-wide general specifications, standards, handbooks, and guidelines
- FAA policy directives
- Established lifecycle processes
- Physical, financial, and human project resources

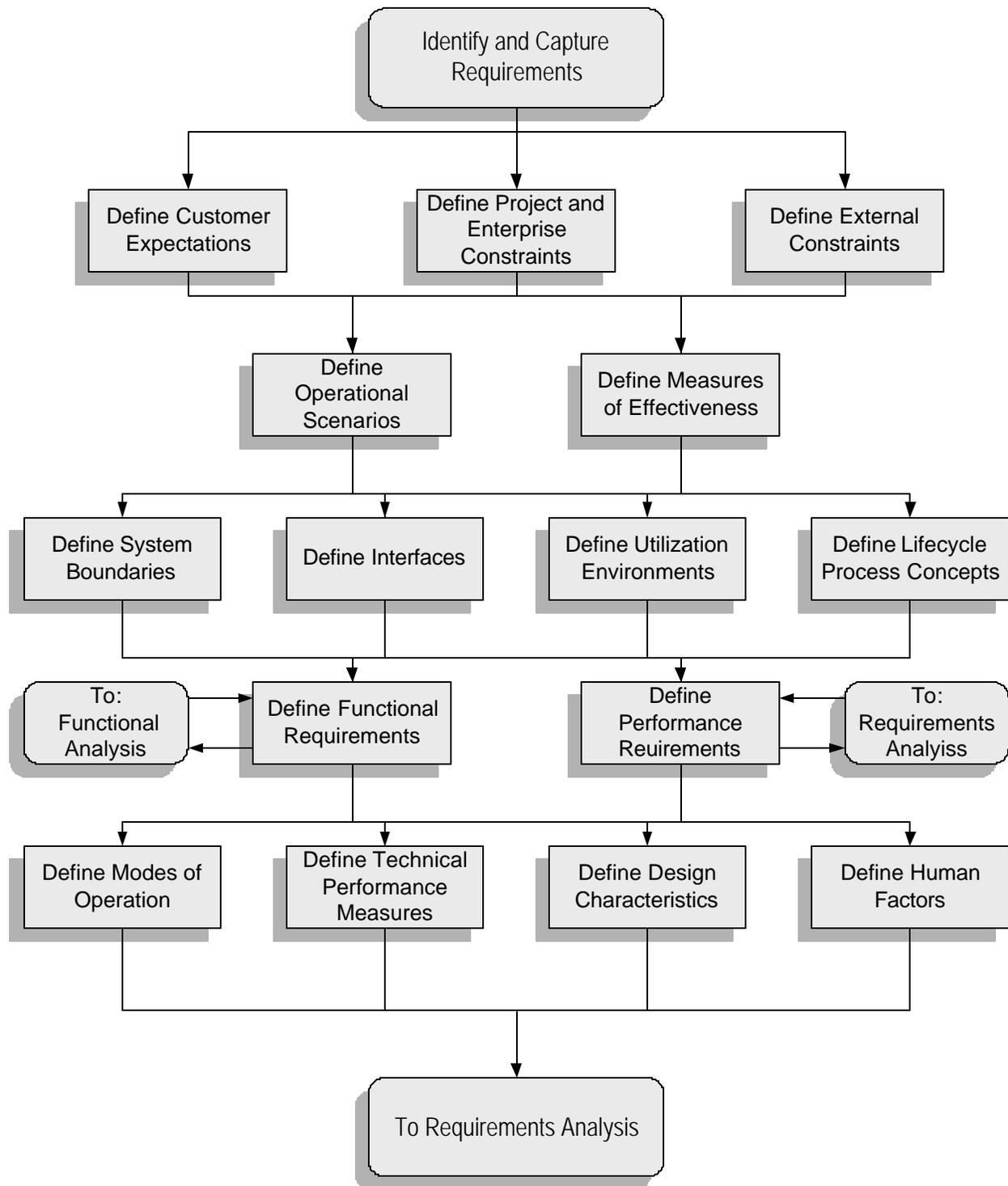


Figure 4.3-4. Identify and Capture Requirements Flow

**4.3.3.1.3.3 Step 1.3: Define External Constraints**

External constraints that impact design solutions or implementation of SE activities are identified and defined. These include:

- U.S. Government and international laws and regulations
- Industry, international, and other general specifications, standards, and guidelines
- ICAO SARPs
- RTCA MOPS and MASPS
- Human-related specifications, standards, and guidelines
- The technology base
- Interfacing systems

#### **4.3.3.1.3.4 Step 1.4: Define Operational Scenarios**

Operational scenarios that define the range of the anticipated system uses are identified and defined. 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.

Data for this step comes from the CONOPS, pPRs and fPRs, and the NAS Architecture.

#### **4.3.3.1.3.5 Step 1.5: Define Measures of Effectiveness**

System effectiveness measures that reflect overall stakeholder needs and operational suitability are defined. Measures of Effectiveness (MOE) are measures of operational effectiveness and suitability in terms of operational outcomes. They identify the most critical performance requirements to meet system-level mission objectives and will reflect key operational needs in the operational requirements document.

Key MOEs may include performance, safety, operability, usability, reliability, maintainability, time and cost to train, workload, human performance requirements, or other factors.

Data for this step comes from the CONOPS, pPRs and fPRs, the NAS Enterprise Architecture, the NAS Level Requirements, and operational scenarios.

#### **4.3.3.1.3.6 Step 1.6: Define System Boundaries**

System boundaries are defined as follows:

- System elements that are under design control and elements that are not
- Expected interactions among system elements under design control and external and/or higher level and interacting systems outside the system boundary

Data for this step comes from any internal, external, policy, or technology constraints; CONOPS; SLMN; pPRs and fPRs; and Functional Analysis.

#### **4.3.3.1.3.7 Step 1.7: Define Interfaces**

The functional and physical interfaces are defined to external or higher level and interacting systems, platforms, and/or products in quantitative terms. Functional and physical interfaces may include mechanical, electrical, thermal, data, communication, procedural, human-machine, and other interactions required. Interfaces may also be considered from an internal/external

perspective. Internal interfaces address elements inside the boundaries established for the system; they are generally identified and controlled by the contractor responsible for developing the system. External interfaces involve entity relationships outside the established system boundaries.

Data for this step is in IRDs, ICDs, Functional Analysis, SLMN, and pPRs and fPRs.

#### 4.3.3.1.3.8 Step 1.8: Define Utilization Environments

Utilization environments for each of the operational scenarios are defined. 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 and that impart minimal risk of death, injury, or acute chronic illness, disability, and/or reduced job performance of the humans who support the system lifecycle. Specifically, weather conditions (e.g., rain, snow, sun, wind, ice, dust, and fog); temperature ranges; topologies (e.g., ocean, mountains, deserts, plains, and vegetation); biological factors (e.g., animal, insects, birds, and fungi); time (e.g., day, night, and dusk); induced factors (e.g., vibration, electromagnetic, acoustic, x-ray, and chemical); or other environmental factors are defined for possible locations and conditions conducive to system operation. It is recommended that effects on hardware, software, and humans be assessed for impact on system performance and lifecycle processes.

Data for this step may be contained in the OSED, Trade Studies, Specialty Engineering analysis, and FAA and military standards, specifications, and handbooks. References to many of these sources appear in Appendix G.

#### 4.3.3.1.3.9 Step 1.9: Define Lifecycle Process Concepts

The outputs of steps 1.1 through 1.8 are analyzed to define lifecycle process requirements needed to develop, produce, test, distribute, operate, support, train, and dispose of system products being procured. These requirements are:

- **Manpower.** The required job tasks and associated workload used to determine the number and mix of humans who support the system lifecycle processes are identified and defined.
- **Personnel.** The experiences, aptitudes, knowledge, skills, and abilities required to perform the job tasks that are associated with the humans who support the system lifecycle are identified and defined.
- **Training.** The instruction education and on-the-job or team training necessary to provide humans and teams with knowledge and job skills needed to support the system lifecycle processes at the specified levels of performance are identified and developed.
- **Human Engineering.** Human cognitive, physical, and sensory characteristics that directly contribute to or constrain lifecycle system performance and that impact human-machine interfaces are identified.
- **Safety.** The System Safety Engineering analysis derives and identifies requirements that are designed to control the risk of identified safety hazards.

#### **4.3.3.1.3.10 Step 1.10: Define Functional Requirements**

Functional requirements for each function of the system as determined by the Functional Analysis process (Section 4.4) are defined, describing what the system will do. The functions identified are used in subsection 4.3.3.1.3.11 to define how well the functions shall be performed and to establish the performance requirements. All system requirements involve both functional and performance aspects that ensure that requirements are complete, consistent, and verifiable.

#### **4.3.3.1.3.11 Step 1.11: Define Performance Requirements**

Performance requirements for each system function are defined. Performance requirements describe how well functional requirements are performed to satisfy the MOEs. These performance requirements are MOPs that are allocated to subfunctions during functional decomposition analysis and that are the criteria against which design solutions (derived from Synthesis (Section 4.5)) are measured. MOPs quantify a technical or performance requirement directly derived from the MOEs. MOPs also reflect key performance requirements in the system specification. MOPs are directly traceable to the MOEs and are used to derive, develop, support, and document the performance requirements that will be the basis for design activities and process development.

There are typically several MOPs for each MOE, which bound the acceptable performance envelope.

#### **4.3.3.1.3.12 Step 1.12: 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., environmental, configuration, and operation) that determine the modes of operation are defined.

Data for this step may come from the NAS or system-level CONOPS, SLMN, OSED, operational scenarios, or Functional Analysis.

#### **4.3.3.1.3.13 Step 1.13: 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 MOPs 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.

Data for this step comes from the CONOPS or the SLMN.

**4.3.3.1.3.14 Step 1.14: Define Design Characteristics**

Required design characteristics that are required to achieve operational suitability (e.g., color, texture, size, anthropometrical limitations, weight, and buoyancy) are identified and defined for the system being procured. Design characteristics that are constraints and that may be changed based on tradeoff analysis (Synthesis (Section 4.5)) are identified.

Data for this step comes from the CONOPS, SLMN, OSED, Functional Analysis, Tradeoff Studies, and FAA and military standards, specifications, and handbooks.

**4.3.3.1.3.15 Step 1.15: Define Human Factors**

Human factor considerations (e.g., design space limits, climatic limits, eye movement, reach ergonomics, cognitive limits, and usability) are identified and defined that affect operation of the system being procured. Human factors that are constraints and may be changed based on tradeoff analysis are identified.

Data for this step comes from the CONOPS, SLMN, OSED, Functional Analysis, Tradeoff Studies, Specialty Engineering analysis, and FAA and military standards, specifications, and handbooks.

**4.3.3.2 Step 2: Analyze and Decompose Requirements**

This activity translates the functional architecture developed in Functional Analysis (Section 4.4) into Primitive Requirement Statements (PRS) that, in turn, are translated into Mature Requirement Statements (MRS).

**4.3.3.2.1 Analyze Requirements**

The functional architecture is the primary input to the Requirements Management process. A functional architecture describes “what” a system will accomplish. The functional architecture consists of functional flow block diagrams (FFBD), timeline sequence diagrams, and functional N-squared (N<sup>2</sup>) charts described in Functional Analysis (Section 4.4). The functional architecture is a living document that increases in level of detail along with the decomposition of requirements. It is recommended that there be a level of functional analysis and corresponding functional architecture for every level of requirements (Table 4.3-1). The Requirements Management process uses the Functional Architecture to derive PRSs.

The Requirements Management process starts with recognition of a need or shortfall in system capability and progresses in increasing detail, as shown in Table 4.3-1.

**Table 4.3-1. Functional Architecture to Requirements Traceability Hierarchy**

Functional Architecture	Requirements
CONOPS →	Service Level Mission Need
Functional Analysis 1 →	Preliminary Program Requirements
Functional Analysis 2 →	Final Program Requirements
Functional Analysis 3 →	System Level Specification
Functional Analysis N →	System Specification to N level

#### **4.3.3.2.1.1 Function to Requirements Transformation**

Function transformation transforms functions into the functional and performance PRSs that describe the system attributes that achieve customers' needs.

A functional architecture (from Functional Analysis (Section 4.4)) is transformed into PRSs through two fundamental methods: (1) a structured analysis methodology called System Functional Requirements Analysis (SFRA) and (2) Functional Architecture Referencing (FAR).

Regardless of the method used, the result is a set of PRSs associated with the system functions.

##### **4.3.3.2.1.1.1 System Functional Requirements Analysis**

SFRA is a structured methodology for developing requirements from a functional architecture. It requires building a matrix of functions and system characteristics then assigning a PRS to each function/characteristic pair if one is needed. The following steps produce a list of functions for which PRSs are developed.

###### **4.3.3.2.1.1.1.1 List Functions**

From the functional architecture, the functions are listed on the vertical axis of a table, such as the example in Table 4.3-2. A tree diagram may be used to assist in creating the function list.

Table 4.3-2. System Characteristic Matrix

Characteristics		Performance		Specialty Engineering				Environment		
		Accuracy	Thermal	Reliability	Safety	Spectrum	Operator workload	Radiation	Lightning	Precipitation
Functions										
Detect AC state vector	Determine aircraft (AC) horizontal location	2	1		3	N	N	N	N	N
	Determine aircraft vertical location	N	N		N	N	N	N	N	N
	Determine aircraft velocity vector	N	N		N		N			
Transmit voice RF	Convert sound to high frequency signal	N	N	N		N	N	N	N	N
	Convert signal to Electromagnetic (EM) wave	N	N	N	N	N		N		N
	Propagate wave through space-time					N		N	N	N
Distribute NOTAM	Encode Notice to Airmen (NOTAM)	N	N		N		N			
	Determine scope	N	N		N		N			
	Transmit NOTAM	N	N		N	N	N	N	N	N

Note: N = PRS number for the specific intersection.

#### 4.3.3.2.1.1.1.1.1 Tree Diagrams

A tree diagram is constructed from the top down. Each subfunction is shown as a branch of the tree. Using the FFBD in Figure 4.4-23 (see Functional Analysis, Section 4.4) as an example, the tree diagram in Figure 4.3-5 was developed as an incomplete example of what the tree diagram might look like. A completed diagram might result in a family tree hierarchy of functions.

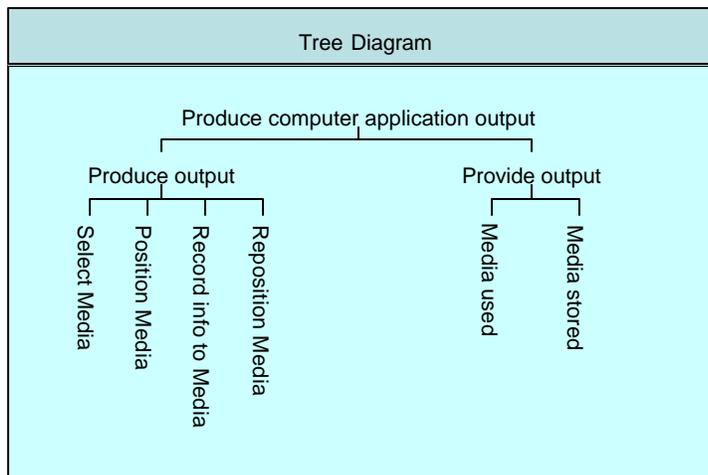


Figure 4.3-5. Tree Diagram Example

#### 4.3.3.2.1.1.1.2 List System Characteristics

System characteristics are developed by identifying all measurable product characteristics perceived as related to meeting customer requirements. These characteristics come from (1) the external inputs described in subsection 4.3.2.1 and (2) analyses conducted in Specialty Engineering (Section 4.8). The characteristics include specialty requirements, constraints, standards, handbooks, management decisions, policies, and legacy requirements. The system characteristics are listed on the horizontal axis of Table 4.3-2. The specific categories and characteristics are unique to and change with each system. The material shown is for illustration only.

#### 4.3.3.2.1.1.1.3 Determine Intersections

This step determines if a need exists to translate a particular function into a PRS. If there is a significant relationship between the function and the characteristic, a PRS number is placed in that cell. "Significant" means that it was determined, using engineering judgment, that the function shall have one or more of the related characteristics in order to meet the customer's need. Wherever there is a number, a unique PRS is required to describe that relationship. The number is associated with the unique PRS that describes the function-characteristic combination. If, this combination is not significant or nonexistent, then a PRS is **not** written for that intersection.

#### 4.3.3.2.1.1.1.4 Develop Primitive Requirements Statements

A PRS for each intersection in the table is developed in accordance with the procedure in subsection 4.3.3.2.1.1.3.

#### 4.3.3.2.1.1.2 Functional Architecture Reference

This method generates PRSs from the standards, handbooks, and Specialty Engineering analyses. The functional PRSs are developed by referencing the functional architecture. Because of the risk of missing critical requirements, it is recommended that this method be used only when there is not enough time to perform an SFRA.

##### 4.3.3.2.1.1.2.1 Derive Primitive Requirements Statement From Standard Sources

A list of PRSs is developed. The PRSs are derived by using the sources described in Specialty Engineering (Section 4.8) and the inputs listed in subsection 4.3.3. The PRSs are developed in accordance with subsection 4.3.3.2.1.2 below.

For example, assume that a reliability analysis derived a requirement that states: "Transmitter Mean Time Between Failures (MTBF) greater than 5,000 op hours." The PRS is listed as a requirement in this list. Table 4.3-3 provides an example.

Table 4.3-3. 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 MTBF greater than 5,000 operating hours	F.3.2.1.1

##### 4.3.3.2.1.1.2.2 Relate Primitive Requirements Statement to Functional Architecture

The functional architecture and existing PRSs are reviewed, and each PRS is assigned to a function in the functional architecture. Each requirement is assigned to a function, and it is recommended that each function have one or more requirements assigned to it.

##### 4.3.3.2.1.1.2.3 Sort the Primitive Requirements Statements by Functional Reference

The list of PRSs developed in subsection 4.3.3.2.1.1.2.2 is sorted or grouped so that requirements allocated to an individual function are together. Table 4.3-4 is an example.

Table 4.3-4. Primitive Requirement Statements List

PRS Number	Primitive Requirement Statement	Functional Reference
126	Transmitter MTBF greater than 5,000 op hours	F.3.2.1.1
34	Transmitter EMI hardened greater than 50,000 volt-meters	F.3.2.1.1
212	Transmitter power less than 10 watts	F.3.2.1.2
6	Transmitted power less than or equal to table 4.3 in HERP standard 6	F.3.2.1.2

PRS Number	Primitive Requirement Statement	Functional Reference
57	Transmitted power less than or equal to table 2.1 in HERF standard 4.4	F.3.2.1.2

Note: EMI= electromagnetic interference; HERP= Hazard of Electromagnetic to Personnel; HERF= Hazard of Electromagnetic Radiation to Fuels

#### 4.3.3.2.1.1.2.4 Write the Functional Primitive Requirements Statement

Once requirements are sorted to functions, the functional PRSs are derived. First, the functional architecture used is appended to the requirements document. Then, for each group of PRSs, a functional PRS is defined in the following manner:

**[Element] functions + as defined in + [Functional Reference (include page and figure number)]**

For the above example table, two functional PRSs are added as shown in Table 4.3-5.

Table 4.3-5. Grouped and Sorted Primitive Requirement Statements List

PRS Number	Primitive Requirement Statement	Functional Reference
126	Transmitter MTBF greater than 5,000 op hours	F.3.2.1.1
34	Transmitter EMI hardened greater than 50,000 volt-meters	F.3.2.1.1
220	Transmitter functions as defined in F.3.2.1.1, page A-26, figure A.2.2	F.3.2.1.1
212	Transmitter power less than 10 watts	F.3.2.1.2
6	Transmitted power less than or equal to table 4.3 in HERP standard 6	F.3.2.1.2
57	Transmitted power less than or equal to table 2.1 in HERF standard 4.4	F.3.2.1.2
221	Transmitter functions as defined in F.3.2.1.2, page A-28, figure A.2.4	F.3.2.1.2

#### 4.3.3.2.1.1.3 Develop Mature Requirements Statements

Once the list of PRSs is developed using either SFRA or FAR, the PRSs are transformed to MRSs in accordance with subsection 4.3.3.2.1.3.

#### 4.3.3.2.1.2 Primitive Requirements Statements

Requirements are first captured as a list of PRSs. A PRS is **a primitive form of a requirement statement that has no punctuation or formal sentence structure and is not written in a formal specification style**. The PRS form is used at this stage to improve the early requirements identification capability by removing the rigor of writing MRSs from the early concept development and to remove the considerable cost of forming mature requirements. Each PRS is uniquely numbered and follows a simple three-part format:

### Name + Relation + Value

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. Numerical requirements use one of six possible relations: less than, greater than, equal to, less than or equal to, greater than or equal to, or between a range of values. For non-numerical requirements, words such as “is,” “be,” and “conforms to” are used as the relation. Table 4.3-6 provides several examples of a PRS.

Table 4.3-6. PRS Examples

Name	Relation	Value	Units
Item Weight	less than or equal to	5120	Kilograms
Item reliability	greater than or equal to	.998	(none)
Item power output	greater than or equal to	100	Megawatts
Item memory margin	greater than or equal to	100	Percent
Item high turn rate	equal to	90	Degree/min
Item screen refresh rate	equal to	20	Frame/sec
Item input power	in accordance with	FAA-G-2100h	(none)

#### 4.3.3.2.1.3 Mature Requirements Statement

Once the PRSs at any level are identified, they are synthesized into MRSs that satisfy the characteristics and attributes of good requirements. An MRS is ***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.***

Requirements characteristics are the principal properties of the MRS (see subsection 4.3.3.2.1.4). Characteristics may apply to individual requirements or to aggregated requirements. A well-defined set of MRSs needs to exhibit certain individual and aggregate characteristics (as described in subsection 4.3.3.2.1.4). Well-defined requirements are clear, concise, and simple. This activity describes (1) how to build requirements from PRSs and (2) the essential characteristics of well-defined requirements.

The result of performing this activity is a baseline set of requirements that satisfies all of the characteristics described herein and that is recorded and maintained over the lifecycle of the product; the set of requirements is also accessible to all parties.

Each PRS is converted to an MRS in the form of specification text. A specification for a system is a published set of requirements that has been properly refined and formatted into more precise language than used for the PRSs. Usually, each PRS becomes a short paragraph when converted into specification text.

Normal specification standards require that the content of a requirements document include complete sentences organized in a particular way. Each requirement statement shall (1) be written in proper grammar, (2) make appropriate use of standard constructs, (3) possess the characteristics and attributes of good requirements, and (4) comply with a specified standard format.

A PRS is converted into an MRS in specification text by adding the characteristics described in the following paragraphs.

- **Paragraph Number.** The type of requirements is identified and a paragraph number is assigned according to the required format. The numbering format is in accordance with the Federal Aviation Administration Acquisition System Toolset (FAST) template or FAA-STD-005 or MIL-STD-961.
- **Paragraph Title.** A paragraph title is identified that is linked to the named or controlled PRS attribute.
- **Subject.** The subject of the requirements is the main topic of the sentence and is linked to the named or controlled PRS attribute.
- **Directive Verb.** The directive verb in the requirement sentence directs the action required and relates the named or controlled attribute to the value. See subsection 4.3.3.2.1.3.1.1 below.
- **Sentence Ending.** The requirements sentence ends with a period and with a commonly used word or phrase that provides a reference to a standard or specification. See subsection 4.3.3.2.1.3.1.2 below.
- **Explanatory Information.** Explanatory, defining, or clarifying information is added after the requirements sentence if necessary to ensure understanding and avoid ambiguity. Explanatory information is often best contained in a glossary; however, if this information is needed, the requirement may not be well formed.

#### 4.3.3.2.1.3.1 Standard Constructs

Standard constructs are used to record requirements to ensure that they have good requirements characteristics.

##### 4.3.3.2.1.3.1.1 Directive Verbs

All requirements documents have directive verbs that denote action, as follows:

- Use the verb “shall” to denote compulsory or mandatory requirement or action that the person being directed is obliged to take. (For example: “The system weight shall be less than 1000 pounds”; or “The contractor shall furnish all facilities and equipment necessary for the tests specified herein.”)
- Use the verb “may” to denote permission or an option that is not obligatory. (For example: “For instruction books of 50 pages or less, multi-ring binding may be employed in lieu of saddle stitching.”)
- Use the verb “will” to denote a declaration of purpose on the part of the government. (For example: “The Contracting Officer will furnish shipping instructions upon request.”)

- The verb “should” is not used in requirements documents. Although the word “should” is used to denote action that is recommended but not obligatory, it may imply duty or obligation in legal usage.

#### 4.3.3.2.1.3.1.2 Commonly Used Words and Phrasings

Certain words and phrases are frequently used in requirements documents. The following rules shall apply:

- Referenced documents requirements are to be written as follows:
  - “...in accordance with Specification (or Standard)...”
  - “...shall be as specified in Specification (or Standard)...”
  - “...shall conform to...”
  - “...conforming to Specification (or Standard)...”
- The phrase “unless otherwise specified” is used to indicate an alternate course of action. The phrase comes at the beginning of the sentence and, if possible, at the beginning of the paragraph. This phrase is limited in its application and used sparingly.
- The term “and/or” shall not be used in requirements documents. The following example conveys the desired meaning: “The panel shall be supported on brackets, pillars, or both.”
- Do not use “minimum” and “maximum” to state limits. Use “no less than” or “no greater than.” This standard construct avoids the ambiguity associated with the limiting values. This does not mean that the words “minimum” and “maximum” may not be used at all, just not to state limits.

#### 4.3.3.2.1.3.1.3 Words and Phrases To Avoid

It is recommended that specific words and phrases be avoided because they are vague, ambiguous, and general. They include “flexible,” “fault tolerant,” “high fidelity,” “adaptable,” “rapid” or “fast,” “adequate,” “user-friendly,” “support,” “maximize,” “minimize,” and “shall have the capability to.”

#### 4.3.3.2.1.4 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. Descriptions of these characteristics follow (with synonyms in parenthesis).

##### 4.3.3.2.1.4.1 Necessary

The stated requirement is an essential capability, characteristic, or quality factor of the product or process. If removed or deleted, it may cause a deficiency that cannot be remedied by other capabilities of the product or process.

This is a primary characteristic that makes a well-defined requirement. Specifications with unnecessary requirements add cost to the product. If a necessary requirement is deleted from the specification, a major need may not be met, even if all other requirements are satisfied.

A good test of necessity is whether the requirement can be traced to higher level documentation. In the case of a system specification, traceability may be verified to user documentation, such as the CONOPS. If there is no parent requirement, the requirement may not be necessary.

#### **4.3.3.2.1.4.2 Concise (Minimal, Understandable)**

The requirements statement includes only one requirement that simply and clearly states only what shall be done, making it is easy to read and understand. To be concise, the requirements statement does not contain any explanations, rationale, definitions, or descriptions of system use, which are used in text analysis and trade study reports, operational concept documents, user manuals, or glossaries. A link may be maintained between the requirements text and the supporting analyses and trade studies in a requirements database so that the rationale and explanations may be referenced.

Determining what constitutes one requirement is a constant struggle in developing requirements and often requires engineering judgment. An example is the requirement in FAA automation systems for a Minimum Safe Altitude Warning/Conflict Alert alarm. This alarm requires an aural alarm and a visual alarm to warn the controller about potential unsafe conditions. Therefore, the question is: Is this one requirement, or does a requirement need to be written for each condition? Multiple requirements in one paragraph are undesirable. Each requirement needs to be managed and verified, and, as such, has an associated cost.

One decision-making approach is to determine how the requirement is to be verified. In the alarm example, it is recommended to verify that the alarms work together; therefore, any test to verify the alarms shall include both the aural and visual alarms, thus combining the aural and visual alarms into one requirement.

#### **4.3.3.2.1.4.3 Implementation-Free (Solution Neutral)**

The requirement states what is required, not how the requirement needs to be met. The requirement states the desired result in functional and performance terms, not in terms of a solution set. It is also recommended that a requirements statement not reflect a design or implementation nor describe an operation, although interface requirements are generally an exception to this rule.

This characteristic of a requirement is perhaps the hardest to judge and implement. At the system level, requirements may be truly abstract or implementation-free. The system requirements have to be synthesized by a system design solution. After a trade study has been conducted between alternatives and a candidate solution has been selected, the system requirements have to be allocated to the elements defined by the system design. This incremental procedure of allocating requirements to the next lower level elements, which depends on system design, means that one level of design is the requirement at the next lower level. The conclusion is that a requirement is implementation-free at the level that it is being specified, but is a result of the design activity at the level above it.

Interface requirements are usually an exception to the implementation-free rule. Interface requirements are specified in IRDs that describe a specific design or an interface or mating part. The interface requirement shall provide complete information so that the two sides of the interface may be designed to work as specified when connected to each other.

#### 4.3.3.2.1.4.4 Attainable (Achievable or Feasible)

The stated requirement may be achieved by one or more developed system concepts at a definable cost. This implies that a high-level conceptual design has been completed or research and development and cost tradeoff studies have been conducted.

This characteristic is a test of practicality of the numerical value or values set forth in a requirement. It signifies that adequate analyses, studies, and trades have been performed to show that the requirement may be satisfied by one or more concepts and that the technology cost associated with the concept(s) are reasonable within program cost constraints.

#### 4.3.3.2.1.4.5 Complete (Standalone)

The stated requirement is complete and does not need further amplification and provides sufficient capability.

This characteristic specifies that each requirement be stated simply using complete sentences. It is recommended that each paragraph state everything required on the topic and that the requirement be capable of standing alone when separated from other requirements.

#### 4.3.3.2.1.4.6 Consistent

The stated requirement does not contradict other requirements and does not duplicate another requirement. The same term is used for the same item in all requirements.

This characteristic of well-defined requirements is usually well understood and does not cause much discussion. However, in a large set of requirements that are not well organized by some clearly defined categories, it may be hard to spot duplications and inconsistencies. Therefore, organizing requirements in accordance with a standard or template is important so that inconsistencies may be identified. It is also important to maintain a glossary of program terms because the meaning of some words is domain dependent.

#### 4.3.3.2.1.4.7 Traceable

It is recommended that each stated requirement be developed in a way that allows it to be traced back to its source. A requirement also needs to identify related requirements (i.e., parents, children, peers) and requirements that might be impacted by changes to it.

This characteristic contributes to completeness by verifying that all requirements have a source or are allocated. It also helps to eliminate unnecessary or missing requirements.

#### 4.3.3.2.1.4.8 Unambiguous

Each requirement shall have **one** interpretation. Language used in the statement shall leave no doubt as to the intended descriptive or numeric value.

This characteristic is difficult to achieve because the language may be unstructured and, in some cases, the same sentence may mean different things to different people. It is helpful to use standard specification language constructs and commonly used words and phrases and to avoid using the constructs cited in subsection 4.3.3.2.1.3.1.3 above.

#### **4.3.3.2.1.4.9 Verifiable (Testable)**

Each requirement shall have an identified means by which to verify that it meets the characteristics established above. The stated requirement is not vague or general but is quantified in a manner that may be verified by one of the verification methods described in Validation and Verification (Section 4.12).

The characteristic of verifiability needs to be considered at the same time that a requirement is being defined. A requirement that is not verifiable is a problem because it involves acceptability of the system. To be verifiable, a requirement shall be stated in measurable terms.

#### **4.3.3.2.1.4.10 Allocatable**

All stated requirements are allocated to the lowest level possible within the physical architecture or assigned to an organization.

This characteristic is important because it helps to eliminate requirements that are not complete, concise, clear, and necessary. If a requirement is not allocatable to the physical architecture, it is probably not a well-formed requirement.

#### **4.3.3.2.1.5 Characteristics of Aggregate Requirements**

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

##### **4.3.3.2.1.5.1 Complete**

The set of requirements is complete and does not need further amplification. The set of requirements has addressed all categories (subsection 4.3.3.2.1.6.3) 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.

##### **4.3.3.2.1.5.2 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.

#### 4.3.3.2.1.6 Additional Requirements Properties

The following subsections describe secondary properties of individual requirements that provide supplementary information about the requirement and its relationship to other requirements and source documents. However, these properties are not essential in all cases. They are typically used in a requirements management database to provide attributes for sorting, classifying, tracing, and managing individual requirements.

##### 4.3.3.2.1.6.1 Requirement Identification

Each requirement is assigned a program-unique identifier (PUI) for identification and tracking purposes. The PUI may be either numeric or alphanumeric and assigned automatically if a requirements management tool is used. The requirement identifier assists in identifying the requirement, maintaining change history, and providing traceability.

##### 4.3.3.2.1.6.2 Level

This property indicates the level at which the specific requirement is applicable in the system hierarchy or WBS. A level I requirement may indicate a top- or system-level requirement; a level II requirement may be a segment or component-level requirement.

##### 4.3.3.2.1.6.3 Requirements Category

Requirements fall into two categories—nonproduct and technical.

##### 4.3.3.2.1.6.3.1 Nonproduct Requirements

Nonproduct requirements are different from technical requirements: They are not imposed on the system or product to be delivered but on the process to be followed by the program. They are usually task oriented. Nonproduct requirements are managed similarly to technical requirements and need to be necessary, concise, attainable, complete, consistent, and unambiguous in the same manner as technical requirements. Nonproduct requirements are often referred to by industry as “Program Requirements.”

Nonproduct requirements are stakeholder or user requirements imposed through contractual vehicles other than specifications, including the contract or contract SOW. Nonproduct requirements include:

- Compliance with Federal, State, or local laws, including environmental laws
- Administrative requirements (e.g., security); stakeholder/vendor relationship requirements (e.g., directives to use government facilities for specific types of work such as tests); and specific work directives (e.g., directives included in the SOW and Contract Data Requirements List (CDRL))

Nonproduct requirements may also be imposed on a program by agency policy, directives, or practice.

#### 4.3.3.2.1.6.3.2 Technical Requirements

Technical requirements apply to the system or service being procured. Technical requirements are described in requirement documents, system specifications, and interface documentation. The types of technical requirements include:

- **Operational Requirements.** These requirements define the interfaces between the end-user and each functional system, maintenance concept and each system, and various other support and related functions or equipment.
- **Functional Requirements.** These requirements identify what the system must do, and not how well the system accomplishes it. They are based on Functional Analysis (Section 4.4).
- **Performance Requirements.** These requirements define how well the product performs its intended function (e.g., accuracy, fidelity, range, resolution, and response times).
- **Interface Requirements.** These requirements identify the performance, physical, and functional requirements associated with the product interfaces (boundary conditions). Interface development is described in Interface Management (Section 4.7).
- **Constraint Requirements.** These requirements identify limitations or restrictions that bound the solution set and may mature into derived requirements. Following are typical constraint requirements.
- **Regulatory Requirements.** These requirements are imposed by statutes or regulations (e.g., the AMS, FAA regulations or directives, Occupational Safety and Health Administration (OSHA) regulations, and Environmental Protection Agency (EPA) directives).
- **Reliability, Maintainability, and Availability/Supportability.** These requirements identify the user's system readiness and mission performance requirements, physical environments, and resources (e.g., personnel, training, and facilities) available to support the mission. Supportability requirements are based on the maintenance concept.
- **Safety Requirements.** These requirements are defined to control the effects of failure conditions, hazards, and/or safety-related functions.
- **Health Hazard Requirements.** These requirements are defined to control the effects of failure conditions, hazards, and health-related functions.
- **Human Performance Interface Requirements.** These requirements define the human system interface(s).
- **Producibility Requirements.** These requirements define the producibility of a product that involves identifying materials, special tools, test equipment, facilities, personnel, and procedures. They identify the manufacturing technology needs, availability of critical materials, long-lead procurement requirements, and manufacturing test requirements, among other aspects.

#### 4.3.3.2 Checklist for Writing and Evaluating Requirements

The following guidelines for writing and evaluating requirements contain representative questions; the list is not intended to be comprehensive.

- **Technical Considerations**
  - Does the requirement state a valid need?
  - Is the requirement verifiable?
  - Has the verification approach been identified?
  - Are the necessary interface requirements stated?
  - Are appropriate data (e.g., tables, figures) included?
  - Are the stated references clearly applicable to the requirement?
  - Is the requirement within the span of knowledge of the requirement owner?
  - Does the requirement have stated values for quantities?
  - Are words that imply a design avoided?
- **Traceability Considerations**
  - Are the applicable parent, child, and peer requirements identified?
  - Are the source and rationale for the existence of the requirement documented?
  - Is the basis for allocation identified?
- **Writing Considerations**
  - Is the requirement stated as a requirement?
  - Is the requirement stated clearly and concisely?
  - Does the requirement represent only one thought?
  - Is the requirement stated positively?
  - Is the requirement void of ambiguous terminology?
  - Is the requirement grammatically correct?
  - Is the requirement punctuated correctly?
  - Is excessive punctuation avoided?

#### 4.3.3.3 Step 3: Derive Requirements

This activity identifies and expresses requirements that result from considering functional analysis, higher level requirements, constraints, or processes. It is recommended that requirements be derived to the lowest practical level before being allocated to the physical

architecture or WBS elements to avoid potential reallocation as the requirement set becomes more detailed.

#### 4.3.3.3.1 Identify Derived Requirements

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. The process translates and traces safety-specific requirements into the system (hardware and software) baseline. The process assesses system safety program requirement tasks for applicability and incorporation into 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.

#### 4.3.3.3.2 Capture Derived 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.

#### 4.3.3.4 Step 4: Allocate Requirements

This activity allocates or assigns requirements to system, personnel, or support activity components and/or appropriate organizational entities. The allocated requirements consist of all requirements, including the breakdown/decomposition of physical characteristics, functions, reliability/maintainability parameters, and performance parameters. Technical requirements are allocated to the physical architecture defined during the Synthesis process via the Requirements Allocation Matrix (RAM). Nonproduct requirements are allocated to the programmatic process via the WBS. Mapping these requirements identifies the owner that has Responsibility, Authority, and Accountability (RAA) for the respective requirement.

#### 4.3.3.4.1 Allocation Process

This process is applied iteratively when new, changed, or derived requirements are generated. One cycle through the Allocate Requirements process is complete when the currently identified requirements have been accurately allocated to the appropriate system, personnel, or support activity component(s). Subsequent analyses, requirement decomposition, and trade studies may produce additional requirements that define the most balanced requirements allocation for the product.

Typically, the requirements are allocated to components of the system hierarchy defined in the physical architecture provided by the Synthesis process (Section 4.5) or to the program hierarchy defined by the WBS. System requirements (including test and verification requirements) are analyzed, refined, and decomposed to ensure complete functional allocation to system, personnel, or support activity components. 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. Allocations early in the requirements management process only designate high-level product components, as a complete design may not have been determined. As the product design matures, the identified requirements may be allocated to lower level components in the physical architecture.

As requirements are identified and allocated at different levels of the product hierarchy, the requirements documents may be produced and formatted to fit the need at that particular level. As the requirements and system hierarchy are iteratively defined to lower levels, each requirement ultimately is allocated to the lowest possible level of the system component. The requirements documents below the system level are simply documents containing the requirements that have been allocated to particular product component(s). The RAM documents the results of the allocation process.

#### 4.3.3.4.2 Hardware and Software Allocation

The requirements allocation process allocates requirements to hardware and software configuration items. Allocation may be continued beyond this level depending on program needs. Software, hardware, and interface specifications are analyzed and refined to ensure that all requirements allocated to software and hardware are adequately addressed and that they do not include inappropriate levels of details. Occasionally, requirements are derived from software requirements; these requirements are documented and maintained.

In addition to allocating requirements to system elements, the process may allocate requirements to incremental allocated baselines. The process establishes functional, performance, and verification requirements for each incremental system or software version.

#### 4.3.3.4.3 Requirements Allocation Matrix

The RAM allocates requirements to components of the physical architecture. Figure 4.3-6 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

The RAM may contain additional information about the requirement and allocations, including:

- Date of inclusion or deletion
- Reference WBS number
- Allocated cost estimate
- CDRL item(s) associated with the requirement
- The requirement owner

Requirement Allocation Matrix			
Functional Architecture		Requirement	Physical Architecture
ID	Name		

**Figure 4.3-6. Requirement Allocation Matrix**

The RAM also 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.

The RAM will be expanded in the Validation and Verification process to define validation characteristics and to describe Requirements verification methodology (i.e., test, analysis, inspection, demonstration).

A requirements management tool may be used to implement the RAM.

#### 4.3.3.5 Step 5: Establish Verification Methodology

This activity develops a verification approach for each requirement documented in the Validation Table received from Validation and Verification, and the Validation Table is transformed into a VRTM. A Verification Requirement specifies the strategy or method used to verify each requirement, and 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. The verification approaches are:

- Inspection
- Analysis
- Demonstration
- Test

A discussion of these methods appears in Validation and Verification (Section 4.12). Figure 4.12-2 is an example of a VRTM. The Test and Evaluation section of the FAST (<http://fast.faa.gov/toolsets/index.htm>) includes specific guidelines for the VRTM.

### 4.3.3.6 Step 6: Manage Requirements Changes

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/program management desires/directives, and any other real or potential changes to the requirements. This activity is conducted according to the Configuration Management process (Section 4.11).

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 projectwide, 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 (Section 4.12). 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.

### 4.3.4 Outputs of Requirements Management

An output of the Requirements Management process is information provided during the process. Outputs are classified as either external or internal according to their destination, as Figure 4.3-7 shows. External outputs are provided to destinations outside SE. Internal outputs are provided to other SE processes described in this manual.

Output requirements are comprehensive and defined for both system products and system processes, including the eight lifecycle functions of development, manufacturing, verification, deployment, operations, support, training, and disposal. Requirements Management is an iterative process that flows from a high level to a low level of requirements (see Figure 4.3-2 above). Therefore, some of the outputs described in the following subsections may be outputs to one stage of the requirements development process and inputs of other stages.

All requirements destinations described are outputs at one point in the process and are captured. The following subsections describe the outputs of the Requirements Management process.

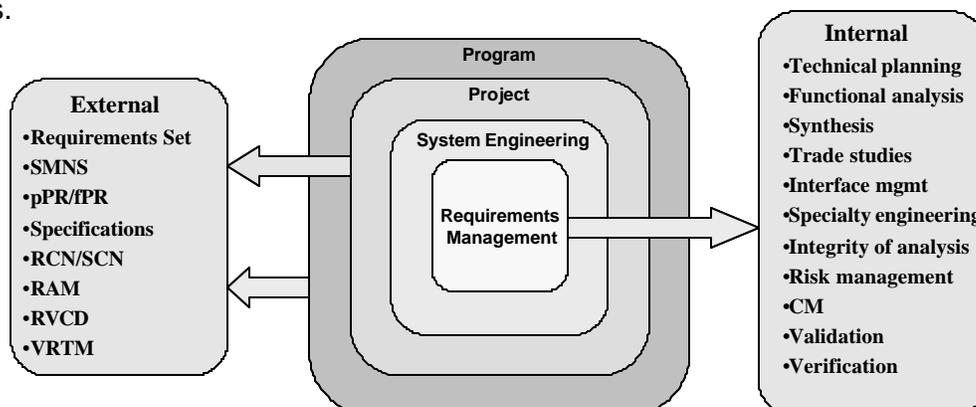


Figure 4.3-7. Output Destinations for Requirements Management

#### **4.3.4.1 External Outputs**

Requirements Management provides external outputs to destinations outside SE boundaries.

##### **4.3.4.1.1 Requirements**

###### **4.3.4.1.1.1 Requirements Documents**

The term “requirements documents” refers to any media that record requirements, either in hardcopy or electronic form. It is a basic rule that all requirements are recorded, including internally generated requirements and those that are generated external to the project. The process does not allow verbal or unwritten requirements.

###### **4.3.4.1.1.1.1 Stakeholder Requirements Documents**

Standard requirements documents from an FAA stakeholder include the SLMN, the pPR, and the fPR. Other organizations use the Operational Requirements Document to communicate requirements. Stakeholders convey requirements through memoranda and other media.

###### **4.3.4.1.1.1.2 Specifications**

Specifications are a standard form of requirements documents. The technical requirements for a system and its elements are documented through a series of specifications as described in this manual. FAA-STD-005e, “Preparation of Specifications, Standards and Handbooks,” describes the requirements for preparing FAA specifications, standards, and handbooks. MIL-STD-961 is the current standard format for FAA specifications required by FAA-STD-005e. FAA specifications were prepared in the MIL-STD-490 format until MIL-STD-490 was canceled, and some legacy specifications remain in that format. However, MIL-STD-490 specifications may continue to be used for reference. Newly prepared specifications are prepared in accordance with FAA-STD-005e.

###### **4.3.4.1.1.1.2.1 Types of Specifications**

The System Specification (Type A) is the single most important engineering specification document, defining the system allocated baseline and including the results from the needs analysis, feasibility analysis, operational requirements and the maintenance concept, top-level functional analysis, and the critical TPMs. 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.

###### **4.3.4.1.1.1.2.1.1 System Specification (Type A)**

Type A includes the technical, performance, operational, and support characteristics for the system as an entity. It includes allocation of requirements of functional areas, and it defines the various functional-area interfaces. The information derived from the feasibility analysis, operational requirements, maintenance concept, and functional analysis is covered. The Type A specification is the FAA-E-XXXX specification described in FAA-STD-005e.

Type A provides the technical baseline for the system as an entity, is written in performance-related terms, and describes design requirements in terms of “whats,” 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.

Type A is the requirements document that FAA uses to procure most systems. It is placed under configuration management before issuance of the system Screening Information Request.

#### **4.3.4.1.1.2.1.2 Development Specification (Type B)**

Type B 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 item of support. Each specification includes the performance, effectiveness, and support characteristics that are required in evolving design from the system level down.

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).

#### **4.3.4.1.1.2.1.3 Product Specification (Type C)**

Type C includes the technical requirements for any item below the top system level that is currently in the 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 CDR.

#### **4.3.4.1.1.2.1.4 Process Specification (Type D) (Rarely Used in FAA Procurements)**

Type D includes the technical requirements that cover a service that is performed on any component of the system (e.g., machining, bending, welding, plating, heat treating, sanding, marking packing, and processing).

A system vendor usually produces the Process Specification in response to the FAA-developed System Specification. The vendor creates it, and the FAA rarely uses it in FAA procurements.

#### **4.3.4.1.1.2.1.5 Material Specification (Type E) (Rarely Used in FAA Procurements)**

Type E includes the technical requirements that pertain to raw materials, mixtures (e.g., paints, chemical compounds), or semifabricated materials (e.g., electrical cable, piping) that are used in the fabrication of a product.

A system vendor usually produces the Material Specification in response to the FAA-developed System Specification. The vendor creates it, and the FAA rarely uses it in FAA procurements.

#### **4.3.4.1.1.2 Requirements Change Notices**

A Specification Change Notice is a formal document specifying that a baselined specification document has been changed.

#### **4.3.4.1.1.3 Requirements Database**

Although requirements can come in the hardcopy formats described above, they are always in the original electronic format in automated requirements management tools.

#### **4.3.4.1.1.4 Requirements Verification Compliance Document**

The RVCD is output to program and project management for program control activities.

#### **4.3.4.1.1.5 Verification Requirements Traceability Matrix**

The VRTM is included as a part of every requirement and specification document. It provides information on the verification and traceability from a requirement to a higher level requirement or to its ultimate source. Validation and Verification (Section 4.12) provides details on this topic.

### **4.3.4.2 Internal Outputs**

The Requirements Management process provides internal outputs to other processes within SE's boundaries and includes outputs to all other SE processes (see Figure 4.3-7 above).

#### **4.3.4.2.1 Integrated Technical Planning**

##### **4.3.4.2.1.1 Planning Criteria**

Planning criteria describing planned activities for the Requirements Management process are output to the Integrated Technical Planning process (Section 4.2). Appendix E details what is to be included in requirements management planning criteria.

##### **4.3.4.2.1.2 Requirements**

The requirements set are an output to the Integrated Technical Planning to use in developing the SEMP and the WBS.

##### **4.3.4.2.2 Functional Analysis**

The requirements set at any stage in the requirements development process are an output to the Functional Analysis process (Section 4.4) for developing the next lower level functional analysis.

##### **4.3.4.2.3 Synthesis**

###### **4.3.4.2.3.1 Requirements**

The requirements set below the SLMN are an output to the Synthesis process (Section 4.5), which allocates requirements to the physical architecture.

###### **4.3.4.2.3.2 RVCD**

The Requirements Verification Compliance Document (RVCD) is an output to Synthesis to ensure system compliance through measurable verification requirements.

#### **4.3.4.2.3.3 Requirements Allocation Matrix**

The RAM is an output to Synthesis for allocation of requirements to the physical architecture.

#### **4.3.4.2.4 Trade Studies**

##### **4.3.4.2.4.1 Requirements**

During the Synthesis process, alternative solutions may be proposed that require analysis by conducting trade studies. The Requirements Management process provides requirements for analysis to the Trades Studies process (Section 4.6).

##### **4.3.4.2.4.2 Constraints**

Constraints that are developed during the Identify and Capture Requirements step may be used in a trade study and are an output to the Trade Studies process (Section 4.6) in addition to requirements.

##### **4.3.4.2.5 Interface Management**

Requirements are provided to the Interface Management process (Section 4.7) at all stages of requirements development so that interfaces are identified and controlled.

##### **4.3.4.2.6 Specialty Engineering**

###### **4.3.4.2.6.1 Requirements**

To perform Specialty Engineering analyses, the system under study is described. Requirements are a key component of any description, and they are an output to Specialty Engineering (Section 4.8).

###### **4.3.4.2.6.2 RVCD**

The RVCD records and provides the verification status of all requirements to Specialty Engineering.

##### **4.3.4.2.7 Integrity of Analysis**

###### **4.3.4.2.7.1 Tools/Analysis Requirements**

Requirements for tools or analysis that are needed during the Requirements Management process are an output to the Integrity of Analysis process (Section 4.9) so that Analysis Criteria may be developed.

###### **4.3.4.2.7.2 Requirements**

Requirements are an output to the Integrity of Analysis process (Section 4.9).

#### **4.3.4.2.8 Risk Management**

##### **4.3.4.2.8.1 Concerns and Issues**

Concerns and Issues related to accomplishing the mission objectives and satisfying stakeholder needs that are discovered during the Requirements Management process are provided to the Risk Management process (Section 4.10) for review and resolution.

The cumulative status of requirements as a result of previous requirements reviews regarding coverage, balance, mutual conflicts, induced constraints, and so forth are analyzed, and Concerns and Issues are identified.

In performing SE, it is possible that potential requirements management problems may surface as Concerns and Issues, which may take many forms, but, mostly, they may be potential risks to the program.

##### **4.3.4.2.8.2 Requirements**

The Requirements Management process identifies requirements to Risk Management (Section 4.10) that are to be analyzed for potential risk. It also produces requirements that are used as mitigations or countermeasures to reduce risk.

#### **4.3.4.2.9 Configuration Management**

The Requirements Management process identifies requirements to the Configuration Management process (Section 4.11) that are to be controlled.

##### **4.3.4.2.10 Validation**

Requirements developed through the Requirements Management process are to be submitted to the Validation process (Section 4.12) to determine if they are complete, concise, and necessary.

##### **4.3.4.2.11 Verification**

###### **4.3.4.2.11.1 Verification Requirements Traceability Matrix**

The Requirements Management process expands the Validation Table into a VRTM with assigned verification methods and submits the VRTM to the Verification process (Section 4.12).

###### **4.3.4.2.11.2 Requirements**

The Requirements Management process submits requirements to be verified to the Verification process (Section 4.12).

##### **4.3.4.2.12 Lifecycle Engineering**

The Requirements Management process submits requirements to Lifecycle Engineering for National Airspace Integrated Logistics System (NAIS) planning to establish objective performance levels for each service element (component) comprising the system at each service or capability delivery milestone.

### 4.3.5 Requirements Management Process Metrics

Performance of this process is measured and recorded on a regular basis. The following metrics, at minimum, 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.
- Unclear, undefined, or ambiguous requirements based on the number of requirements 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

### 4.3.6 Tools

#### 4.3.6.1 Requirements Tool Characteristics

It is recommended that the database be capable of identifying (i.e., attributes and relationships) and presenting (e.g., internal queries, standard and project-unique reports) the following types of information:

- **Requirements documentation**—statements of the requirements, status, requirement type, rationale, and history (including data configuration control) regarding each requirement, and presenting the requirements in an appropriate user-defined format (e.g., requirement documents, and specifications)
- **Traceability**—linking requirements to their parent, child, and peer requirements, resulting in user-defined requirement traceability matrices
- **Allocation**—linking requirements to the product hierarchy, resulting in user-defined requirements allocation documents
- **Verification**—linking the requirement to specific verification approach attributes, resulting in requirements verification and compliance documents
- **Traceability Impact Assessment**—assessing the impact of proposed changes to the requirement, product, and verification hierarchies
- **Compatibility**—communicating (minimum of import and export capabilities) with other automated tools

#### 4.3.6.2 Requirements Management Software

Deciding whether to use an automated requirements tool for documenting requirements and related information depends on a variety of factors (e.g., size and complexity of the program, number of requirements, budget). There are multiple automated software tools in the marketplace that adequately store and retrieve the requirements and their traceability. A program's tool maintains two-way traceability, from system specifications to hardware and software configuration item specifications. It can be integrated into an overall SE tool suite so that data moves seamlessly between applications.

For small programs, a spreadsheet may be more than adequate to document and control the requirements set. As a program grows and becomes more complex, a tool designed for requirements management may be necessary.

#### 4.3.6.3 Requirements Database

All program personnel have access to the requirements information. Users may have access to either the database itself or to database-derived documentation. A program decision is made concerning the availability and changeability of the requirements data. All personnel may be trained in using the requirements management tool or database, or a select group may manipulate the database and use a distribution media (e.g., intranet Web site or paper) to disseminate the information and collect comments and changes.

#### 4.3.7 References

1. Blanchard, B. *System Engineering Management*. 2nd edition. New York, NY: John Wiley & Sons, Inc., 1998.
2. Defense Systems Management College. *Systems Engineering Fundamentals*. Fort Belvoir, VA: Defense Systems Management College Press, 2001.
3. *FAA Directives System*. FAA Order 1320.1D Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, 26 August 1992.
4. Grady, Jeffrey. *System Requirements Analysis*. New York, NY: McGraw Hill, 1993.
5. Hooks, Ivy. *Guide for Managing and Writing Requirements*. Houston, TX: Compliance Automation, Inc., 1994.
6. *IEEE Standard for Application and Management of the Systems Engineering Process*. IEEE Std 1220-1998. New York, NY: Institute of Electrical and Electronic Engineers, 1998.
7. Kar, Philip, and Michelle Bailey. *Characteristics of Good Requirements*. Paper at the 6th INCOSE Symposium 2000. Houston, TX: Compliance Automation, Inc.
8. *National Airspace System Architecture*. Version 5. Washington DC: U.S. Department of Transportation, Federal Aviation Administration.
9. *National Airspace System Concept of Operations and Vision for the Future of Aviation*. Washington DC: RTCA, Inc.
10. *National Airspace System Design Specification*. NAS-DD-1000. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration.
11. *National Airspace System Engineering Management Plan*. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration.
12. *National Airspace System Master Configuration Index: Subsystem Baseline Configuration and Documentation Listing*. NAS-MD-001. Revision 17. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, July 1999.
13. *National Airspace System Systems Requirements Specification*. NAS-SR-1000. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration.
14. *National Airspace System Systems Specification*. NAS-SS-1000. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration.

15. *Preparation of Specifications, Standards and Handbooks*. FAA-STD-005e. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration.
16. Sage, A., and Rouse, W., eds. *Handbook of Systems Engineering and Management*. New York, NY: John Wiley & Sons, Inc., 1998.
17. *Standard Practice for Defense Specifications*. MIL-STD-961E. Washington DC: U.S. Department of Defense, 1 August 2003.
18. Young, R. *Effective Requirements Practices*. New York, NY: Addison-Wesley, 2001.

#### 4.4. Functional Analysis (*Satisfies EIA 731 FA 1.2 and iCMM PA 4*)

This section details the preferred approach of the Federal Aviation Administration (FAA) to performing Functional Analysis. Functional Analysis is the System Engineering (SE) process that translates stakeholders' needs into a sequenced and traceable functional architecture. This process of analyzing functions provides SE with a functional system description that becomes a framework for developing requirements and physical architectures. Using the Functional Analysis process significantly improves synthesis of design, innovation, requirements development, and integration. The Functional Analysis process provides two key benefits to SE: It discourages single-point solutions, and it describes the behaviors that lead to requirements and physical architectures. Figure 4.4-1 lists the essential elements of Functional Analysis, including the inputs, processes providing input (providers), process tasks, outputs, and processes receiving outputs (customers).

##### 4.4.1. Introduction to Functional Analysis

Systems may be described from at least two different perspectives. One perspective sees the system as a physical architecture with elements that interact with themselves and the system environment in accordance with a predefined process to achieve the system mission. Another view describes the system by the functions that it performs. A system is intended to satisfy predefined functions, with the highest level function defined as the stakeholder need (also the ultimate system requirement or ultimate system function). A *function* is a characteristic action or activity that needs to be performed to achieve a desired system objective (or stakeholder need). A *function name* is stated as 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." The function occurs within the system environment and is performed by one or more system elements composed of hardware, software, firmware, people, and procedures to achieve system operations. In Functional Analysis, because a function may be accomplished by more than one system element, functions cannot be allocated. Rather, functions are used to develop requirements, which are then allocated to solutions in the form of a physical architecture.

When systems that are being developed radically differ from current ones, the "form follows function" approach is applied. The highest level function, the stakeholder need, is decomposed into lower levels of needed functionality. The functional description is translated into the physical realm by defining requirements from the functions and assigning the requirements to objects within a physical architecture. While, theoretically, function names could be allocated to specific physical architecture entities directly, most times, some combination of two or more architectural entities accomplishes one function.

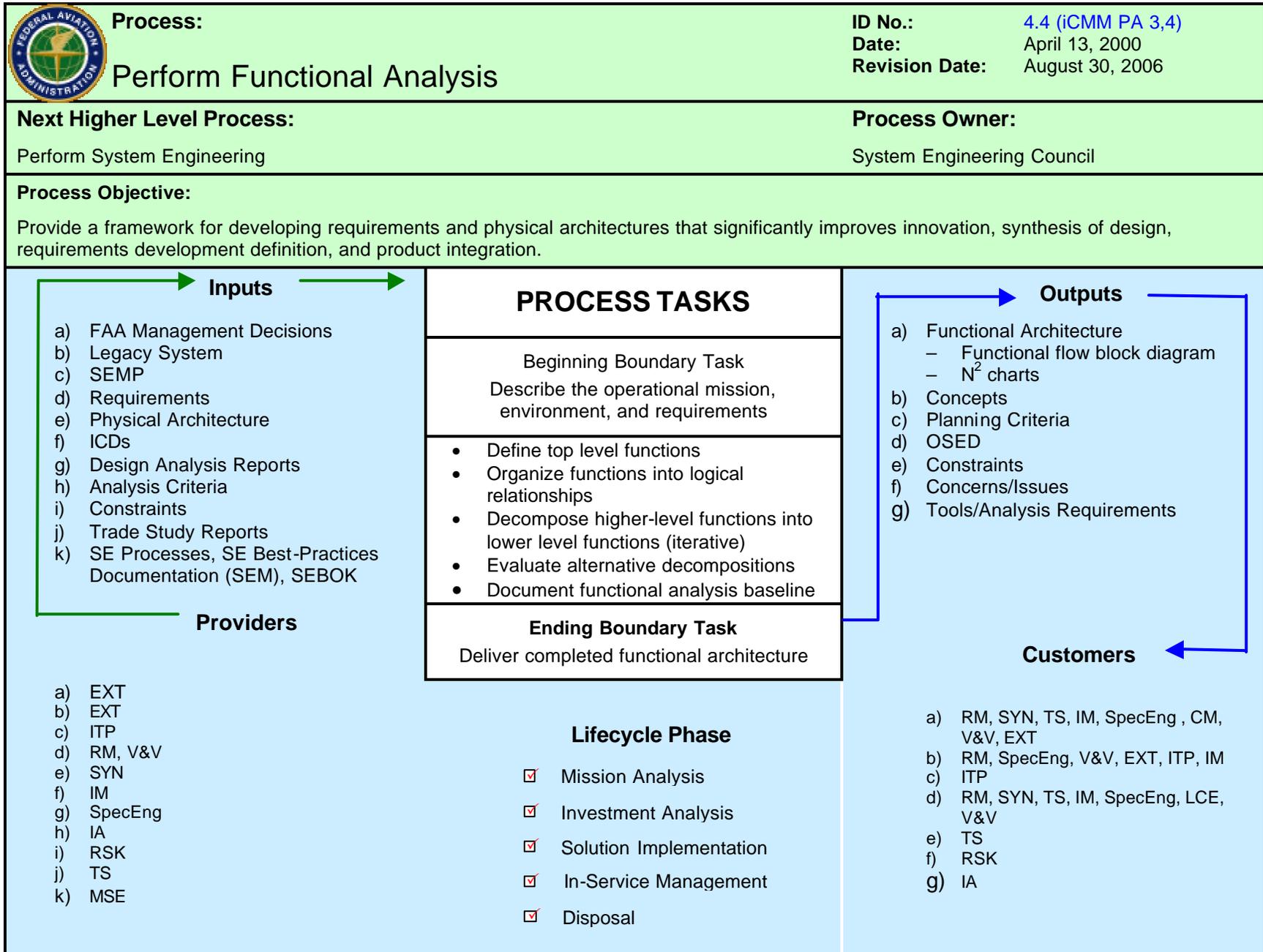


Figure 4.4-1 Functional Analysis Process-Based Management Chart

#### 4.4.1.1. Functional Analysis Objectives

The Functional Analysis process helps to ensure that:

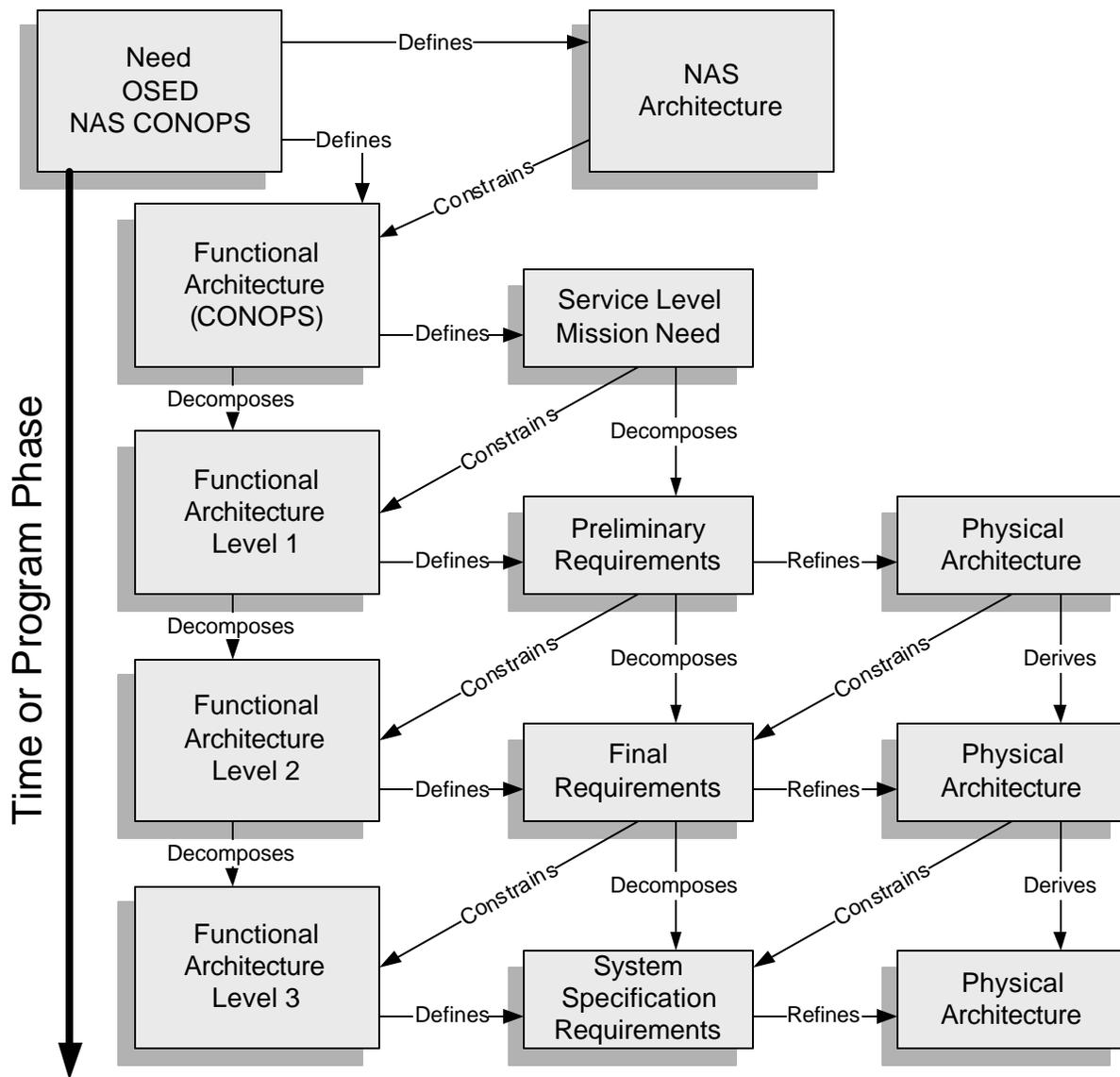
- All facets of a system's lifecycle, as illustrated in Figure 4.4-1, are covered, from development to production, operation, deployment, and disposal
- All functional elements of the system are described, recognized, and defined
- All system concepts and requirements for specific system functions are related
- Requirements definition is improved
- Product integration is improved
- New and innovative designs and solutions are incorporated

#### 4.4.1.2. Process Overview

The Functional Analysis process examines a system's functions and subfunctions that accomplish the system's operation or mission. It describes *what* the system does, not *how* it does it. Functional Analysis is conducted at the level needed to support later synthesis efforts, with all operational modes and environments included. Each function required to meet the operational needs of a system is identified, defined, and organized into a functional architecture that is used to define system requirements. A functional architecture is a hierarchical arrangement of functions and interfaces that represents the complete system from a performance and behavioral perspective. The process moves to a greater level of detail as the identified functions are further decomposed into subfunctions, and the requirements and physical architecture associated with those functions are decomposed as well. Functional decomposition reduces complexity by allocating functionality and interfaces to more readily understood and managed sublevel functions. This process is repeated until the system is completely decomposed into basic subfunctions, and each subfunction at the lowest level is defined by a valid set of requirements. The interfaces between each of the functions and subfunctions are fully defined, as are the interfaces to the environment and external systems. The functions and subfunctions are arrayed in a functional architecture to show their relationships and internal and external interfaces. **Figure 4.4-2** illustrates the Functional Analysis process flow.

Functions shall be:

- Arranged in their logical sequence
- Clearly defined in their inputs, outputs, and functional interfaces (internal and external)
- Traceable from beginning to end conditions
- Analyzed, determined, and defined for time-critical requirements
- Successively established from the highest to lowest level for each function and interface
- Defined in terms of what needs to be accomplished in verb-noun combinations without describing *how* it is to be accomplished ("implementation free")
- Traceable downward through successive functional decompositions



**Figure 4.4-2. Requirements Management Process Flow**

The Functional Analysis process is conducted in conjunction with Requirements Management (Section 4.3) and Synthesis (Section 4.5) to:

- Define successively lower level functions required to satisfy higher level requirements and to define increasingly detailed sets of the functional architecture
- Define mission- and environment-driven performance requirements and determine that higher level requirements are satisfied
- Flow down performance requirements and design constraints
- Refine the definition of product and process solutions

#### 4.4.1.3. Iterative Process Dependencies

Functional Analysis is an iterative process that works with and depends on the Requirements Management and Synthesis processes. Functional Analysis begins with a high-level

requirement (e.g., a newly identified 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.

Starting with the latest National Airspace System (NAS)- and/or Service-level Concept of Operations (CONOPS), the current NAS-level physical architecture, and the newly identified need, the initial Functional Analysis produces concepts (e.g., a Concept of Use (CONUSE)); see subsection 4.4.5.2 below) for the system (new or modified) that will eventually meet the need. The functions described in a CONUSE, along with identified nonfunctional requirements (e.g., environmental), are used in the Requirements Management process to formally document the new high-level requirement (e.g., in a Service-level mission need statement). At this point in the process, requirements lack sufficient detail to synthesize a physical architecture, so the Synthesis process is not performed.

After completion of the service-level mission need statement during the first pass through the requirements process, the concepts are further decomposed using the Functional Analysis process, as constrained by the requirements. The results of this stage of Functional Analysis are typically captured via one or more diagramming techniques (e.g., functional flow block diagramming (FFBD) and N-squared ( $N^2$ ) diagramming). This stage of Functional Analysis produces the preliminary draft of the functional architecture and is used to further develop requirements that are documented in the preliminary Program Requirements (pPR). The pPR is used to define the initial draft of the physical architecture during the Synthesis process. The process is repeated until the physical architecture at the lowest system specification level is derived.

At any time during the process, the functions and requirements at a higher level can be reworked as necessary. These changes will then spread downward through the process until the lower levels reflect the changes.

#### **4.4.2. Inputs to Functional Analysis**

The stakeholder's needs will be the primary input at the highest level of Functional Analysis for the FAA. This requirement (i.e., a newly established need) is the ultimate function and is used as the catalyst for developing concepts. The initial or highest level concepts for a new or modified system are usually documented in a CONUSE. A CONUSE is primarily a textual document of the results of high-level Functional Analysis efforts. It is usually derived solely from the user's perspective. It is recommended that the CONUSE serve as a baseline for the more detailed Functional Analyses to follow. (Subsection 4.4.5.2 below gives more information on the CONUSE.) Inputs into detailed Functional Analysis will vary depending on the scope of a given effort and the iteration of the process.

Lower level Functional Analysis efforts will have as their input the Service-level mission need, higher level functional and physical architectures, and, eventually, for subsequent iterations of the process, the pPR or fPR. If the output of the Requirements Management (Section 4.3) task is incomplete, the Functional Analysis task reveals missing requirements and helps to refine or clarify other requirements. Additional input includes feedback from stakeholder interviews and functional architecture reviews.

The following is a more comprehensive list of the Functional Analysis inputs:

- FAA management decisions
- Information on legacy systems
- NAS-level (and program, if available) System Engineering Management Plan

- Requirements, such as those contained in the Service-level mission need statement (including defined NAS capability shortfalls and/or needs), requirements documents, specifications, and standards
- Existing physical architectures
- Higher level functional architectures and concepts
- Information on interfaces, including Interface Control Documents
- Design Analysis Reports
- Analysis Criteria
- Constraints

#### **4.4.2.1. FAA Management Decisions**

Management decisions that the national, department, or agency level imposes on the system are identified and analyzed for their impacts on the system's intended functionality. Also, program-level management decisions may introduce constraints related to reusing previously developed hardware and software with existing functionality that must be incorporated.

#### **4.4.2.2. Legacy System**

Two cases exist in which legacy system information is required as an input to the Functional Analysis process. Case one involves completely replacing an existing system, which means that its existing functionality must be maintained in the follow-on system. Case two involves developing a new higher level system that will incorporate one or more legacy systems (i.e., the legacy system becomes a subsystem within a new higher level system). In either case, lack of any functional documentation for the legacy system may require some reverse engineering to identify the legacy system's functionality and thus derive all the benefits gained from using Functional Analysis.

#### **4.4.2.3. System Engineering Management Plan**

This plan lays out the specific system engineering tasks and responsibilities for an organization or program and thus drives Functional Analysis planning efforts.

#### **4.4.2.4. Requirements**

The initial high-level requirement, which represents any stakeholder's desire for a new capability or change to an existing system, is often expressed as a "need." Every need requires validation to ensure that it truly addresses a shortfall in capability and/or that it has the possibility to capitalize on a new technological opportunity. This validated high-level requirement initiates the Functional Analysis process and is formally documented in the Service-level mission need as defined in the Acquisition Management System.

Lower level requirements are decomposed from the initial high-level requirement(s) in the pPR, fPR, and specifications and are an input to the Functional Analysis process that constrains or bounds the lower level Functional Analysis efforts.

#### **4.4.2.5. Physical Architecture**

A system's physical architecture represents the solution set to defined requirements. A physical architecture is a hierarchical arrangement of hardware and/or software components along with associated interfaces depicting the physical definition of the system. Lower level Functional Analysis work is constrained by a higher level physical architecture. For example, if a radar is

the solution to an aircraft tracking requirement (rather than an optical or thermal tracking device), then the lower level tracking functions will be different than those functions associated with a different solution (i.e., a different physical architecture).

#### **4.4.2.6. Interface Control Documents**

Interface Control Documents (ICD) provide the “as-built” solution information to interface with other systems.

#### **4.4.2.7. Design Analysis Reports**

Design Analysis Reports (DAR), which document the results of a specific Specialty Engineering analysis, including the rationale, are inputs to the Functional Analysis process. Each DAR contains a description of the system's special characteristics, a list of existing requirements that have undergone the Validation and Verification process (Section 4.12), residual risks, and candidate requirements found as a result of the analysis. The rationale supplementing the DARs includes the scope, ground rules, assumptions, constraints, methods, and tools applicable to the analysis.

#### **4.4.2.8. Analysis Criteria**

If the Functional Analysis process requires an analysis or selection of a tool, analysis criteria are captured for that analysis or selection. The analysis criteria for conducting a required analysis are in the Analysis Management Plan.

#### **4.4.2.9. Constraints**

Constraints are internal or externally imposed boundary conditions that place limits on the system.

Constraints can stem from various areas, including:

- Management decisions
- Specifications, standards, handbooks, and guidelines
- Policy directives
- Established lifecycle processes
- Physical, financial, and human project resources
- Design limitations

#### **4.4.2.10. Trade Study Reports**

In the Functional Analysis process, multiple functional architectures may be produced to accommodate alternatives in accordance with various combinations of constraints. These architectures are then compared using the Trade Studies process (Section 4.6) with the design criteria from Synthesis in order to select the functional architecture that most effectively meets mission objectives. The Trade Study reports provide results of the Trade Studies process comparisons to the Functional Analysis process.

#### **4.4.2.11. SEM Revisions**

The System Engineering Manual (SEM) and its revisions are not in and of themselves direct inputs into the Functional Analysis process. However, they do impact the actual conduct of the process. As the process is practiced, feedback from users may necessitate changes to the process. The SEM documents these changes.

### 4.4.3. FAA's Preferred Diagramming Techniques

The FAA prefers using the complementary FFBD and  $N^2$  diagramming techniques for modeling the functional behavior of a system. A complete functional model must depict both the “control” and “data” aspects of the system simply. The simple FFBD technique captures the control (or the logical) environment of a system, while the  $N^2$  diagramming captures the data environment of a system. Subsections 4.4.3.1 and 4.4.3.2 provide a standardized approach to these preferred techniques and lay the foundation for presenting the actual Functional Analysis process tasks in subsection 4.4.4.

To be sure, there are other diagramming techniques (see subsection 4.4.6.2)—each with its own merits—that can be used (when tailoring has been approved) to capture Functional Analysis results. However, these techniques are more visually complex, or they fail to completely capture enough of the information to completely model a system's functionality.

#### 4.4.3.1. Functional Flow Block Diagrams

The FFBD is a multi-tier, time-sequenced, step-by-step diagram of the system's functional flow. FFBDs usually define the detailed, step-by-step operational and support sequences for systems, but they are also used effectively to define processes in developing and producing systems. The software development processes 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 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 from left to right show 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, an “eat food” function logically would not begin until a “cook food” 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 “eat food” function is enabled once the “cook food” function is completed, and once it receives the “prepared food” as input. This second aspect—triggering a function—speaks to the “data” environment, which the  $N^2$  diagram captures (see subsection 4.4.3.2 below).

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.

##### 4.4.3.1.1. 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 4.4-3 above. The figure also depicts how to represent a reference function, which provides context within a specific FFBD. (See Figure 4.4-9 for an example regarding use of a reference function.)

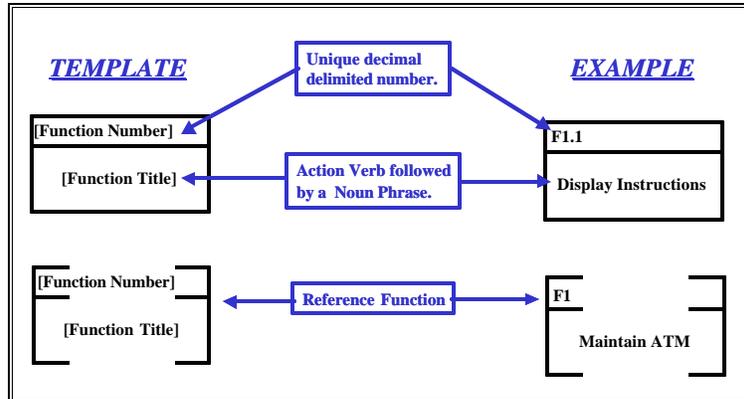


Figure 4.4-3 Function Symbol

4.4.3.1.2. Directed Lines

A line with a single arrowhead shall depict functional flow from left to right (see Figure 4.4-4. Directed Lines

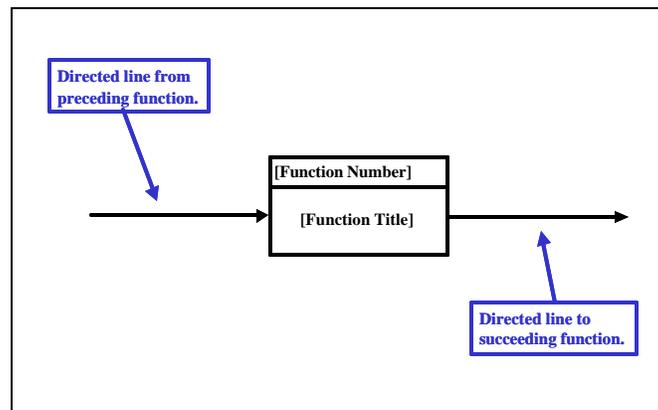


Figure 4.4-4. Directed Lines

4.4.3.1.3. 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 4.4-5). 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.

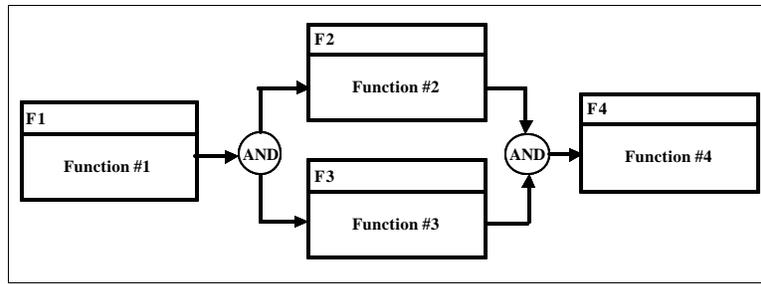


Figure 4.4-5. "AND" Symbol

**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 4.4-6). 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.

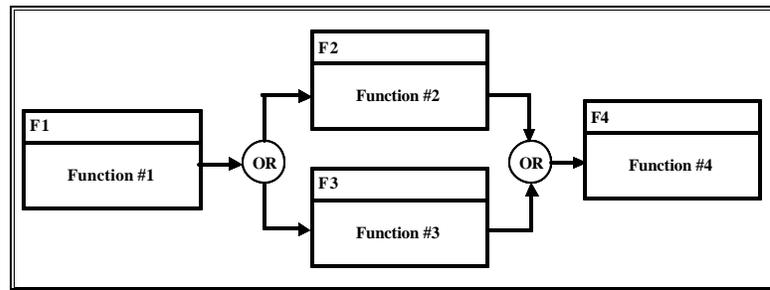


Figure 4.4-6. "Exclusive OR" Symbol

**Inclusive OR:** A condition in which one, some, or all of the multiple preceding or succeeding paths are required. Figure 4.4-7 depicts **Inclusive OR** logic using a combination of the **AND** symbol (Figure 4.4-5) and the **Exclusive OR** symbol (Figure 4.4-6). Read Figure 4.4-7 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.

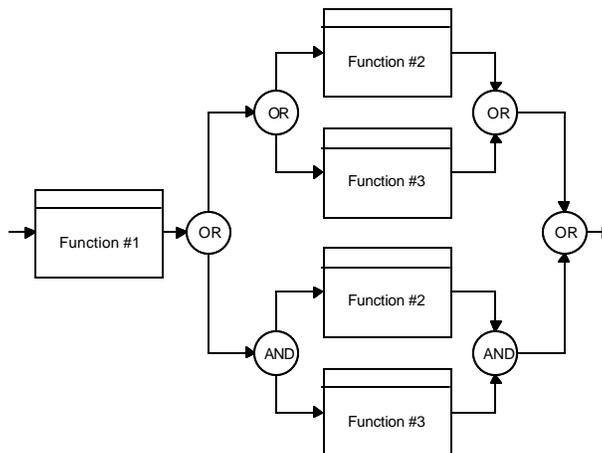


Figure 4.4-7. "Inclusive OR" Logic

#### 4.4.3.1.4. 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 4.4-8 and Figure 4.4-9 present the data in an FFBD. Figure 4.4-9 is a decomposition of the function F2 contained in Figure 4.4-8 and illustrates the context between functions at different levels of the model.

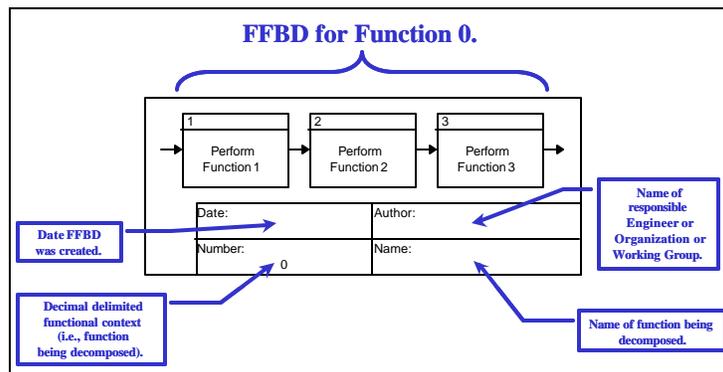


Figure 4.4-8. FFBD Function 0 Illustration

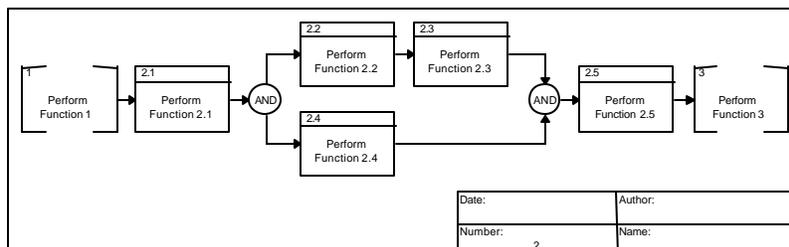


Figure 4.4-9. FFBD Function 2 Illustration

#### 4.4.3.2. N-Squared 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  $N \times N$  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  $F1 \downarrow F2$  in Figure 4.4-10 indicates data flowing from function F1 to function F2; the symbol  $F2 \uparrow F1$  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 4.4-10 illustrates directional flow of interfaces between entities within an  $N^2$  diagram. (In this case, the entities are functions.)

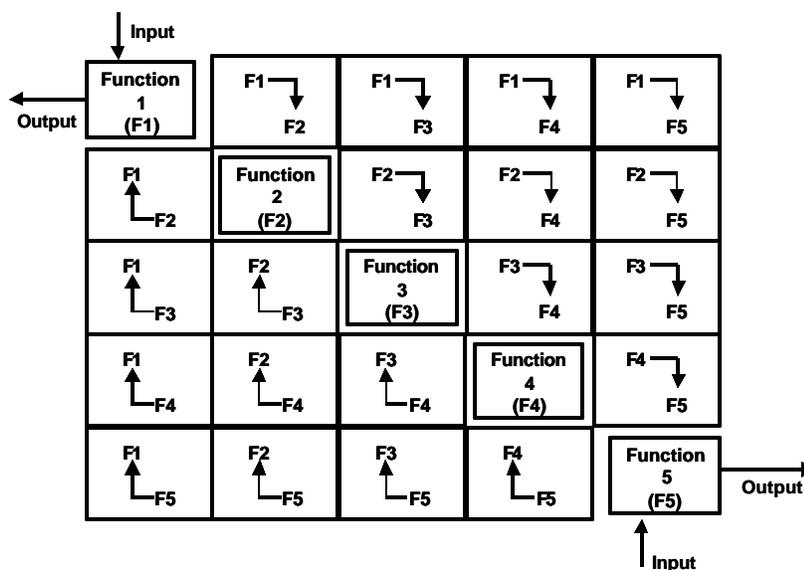


Figure 4.4-10.  $N^2$  Diagram

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 4.4-11 presents the information in an  $N^2$  diagram, which complements the FFBD (Figure 4.4-8 above). Notice that in this illustration, there are no data elements or triggers. Figure 4.4-9 is a decomposition of the function F2 in Figure 4.4-11 and illustrates the context between functions at different levels of the model. Figure 4.4-12 complements the FFBD illustrated in

Figure 4.4-9 and is an example of the diagram's appearance when cells are populated with data.

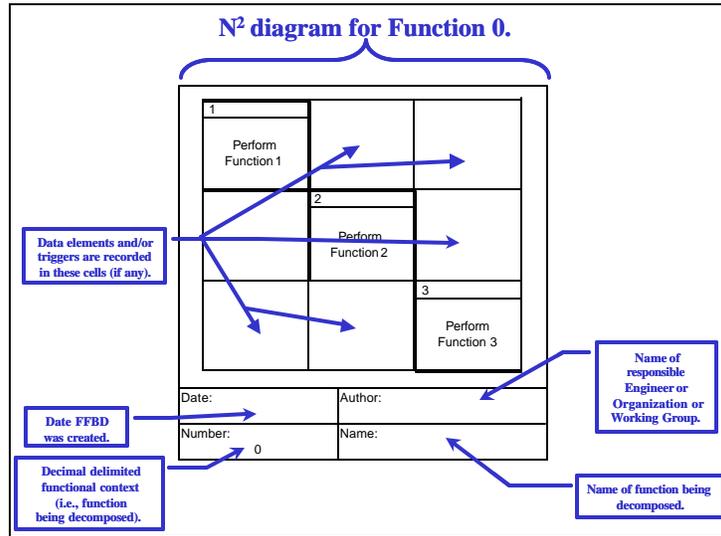


Figure 4.4-11. N<sup>2</sup> Diagram Illustration #1

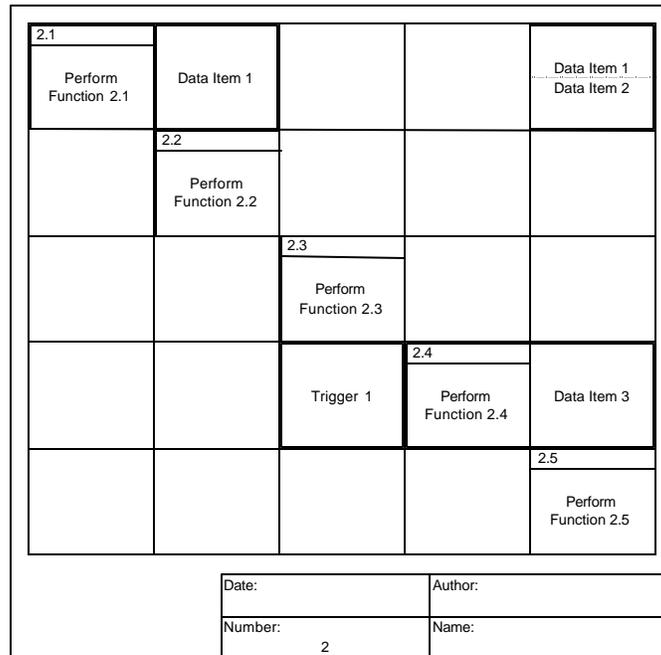


Figure 4.4-12. N<sup>2</sup> Diagram Illustration #2

#### 4.4.4. Functional Analysis Process Tasks

Figure 4.4-1 (Process-Based Management Chart) summarizes the Functional Analysis process, including the five major process tasks. The rest of this section describes these processes within the context of using the FAA's preferred FFBD and N<sup>2</sup> diagramming techniques. These are the same tasks used in developing concepts or an Operational Services and Environmental

Description (OSD), or for alternative diagramming techniques. In generating concepts or an OSD, one simply develops textual descriptions rather than diagrams. (See subsection 4.4.5.2 below for more details.)

To facilitate one’s understanding of the Functional Analysis tasks, a functional architecture will be developed from an oversimplified high-level requirement for an autopilot, as follows:

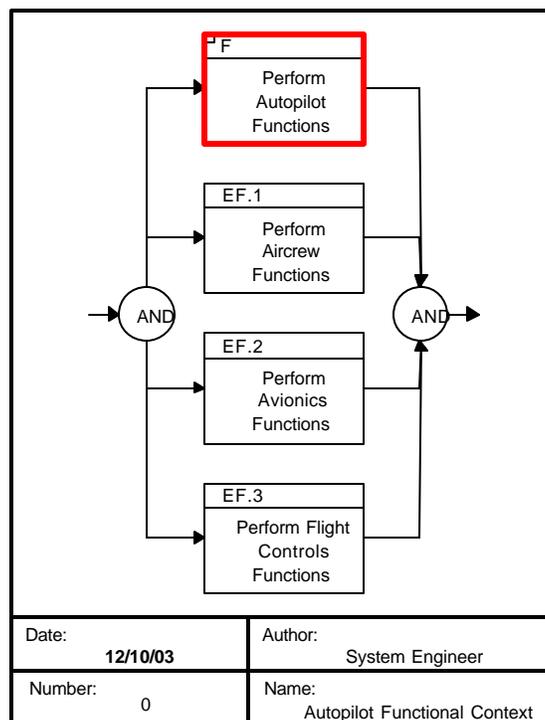
“Avionics shall automatically maintain current altitude, current airspeed, and level attitude upon pilot request.”

**4.4.4.1. Task 1: Define Top-Level Functions (From Inputs)**

**Task 1.1 Bound the Problem Space**

To define the problem space from a functional standpoint, one must first review all existing inputs to obtain a complete understanding of the top-level missions/functions, environments, requirements, imposed constraints, and boundaries. This understanding of all possible inputs ensures that one will consider the future system’s relationship to its environment and external systems during development of the primary functions.

Figure 4.4-13 and Figure 4.4-14 consider the need and create the top-level function called “Perform Autopilot Functions” (outlined in red in the figures). This primary function is named using the guidelines and naming convention described in the “Introduction to Functional Analysis” (subsection 4.4.1) and is the ultimate function that must be fulfilled to successfully accomplish the system’s mission. For the purpose of illustration, it is assumed that analysis of other inputs enabled the bounding of the system as captured in the two figures. The boundary is the red outline of function F, “perform autopilot functions.” Decomposition of function F will generate all of the functions required within the boundaries of the system to meet the given need. The three other functions—EF.1, EF.2, and EF.3—are external functions.



**Figure 4.4-13. Autopilot Functional Context FFBD**

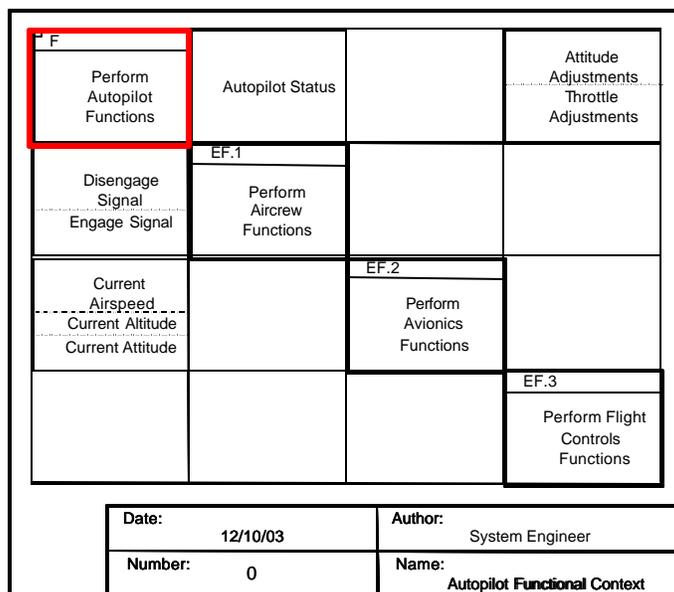


Figure 4.4-14. Autopilot Functional Context N2 Diagram

Note that depending on the iteration of this process, there may exist a higher level FFBD and N<sup>2</sup> that will serve as the functional context diagram. Additionally, due to concurrent engineering efforts, lower level Functional Analysis work may occur in parallel with higher level Functional Analysis work. The lower level working groups are responsible for coordinating their efforts with the higher level working groups.

### Task 1.2 Document Assumptions

Where input is lacking, assumptions and issues are documented (see Appendix D) to validate via stakeholders as soon as possible. In reality, if the input was only the need stated for the autopilot example, then essentially all the external functions and data elements in Figure 4.4-13 and Figure 4.4-14 would need to be captured as assumptions and eventually validated.

### Task 1.3 Identify Stakeholders

At a minimum the stakeholders shall include:

- The system engineer(s) responsible for the associated service or system
- The system engineer(s) responsible for related cross-cutting disciplines
- The lead for any higher level Functional Analysis efforts

In the autopilot example, stakeholders may include pilot organizations, avionics engineers, and human factors engineers.

### Task 1.4 Decompose Top-Level Function

In this task, one must identify and document the highest level functions required to execute the top-level function. The best way to identify these functions is to analyze the system's inputs and outputs captured in the functional context diagrams (see Figure 4.4-13 and Figure 4.4-14). Performing this "thread" analysis, one asks the question, "What must the system do when it receives a specific input?" And, "What must the system do to produce the required output?"

The main criterion for completing this decomposition is development of a comprehensive list of the highest level functions associated with the current iteration of the process that the system

must perform to meet its mission. The list need not be in logical order. Regarding the autopilot example, assume that the following functions are identified:

- Check for aircrew command
- Record baseline altitude
- Record baseline airspeed
- Receive current altitude
- Receive current airspeed
- Record current airspeed as baseline
- Record current altitude as baseline
- Provide autopilot status
- Compare current altitude to baseline altitude
- Compare current airspeed to baseline airspeed
- Make attitude adjustment
- Make throttle adjustment

### Task 1.5 Create a Functional Hierarchy

In Task 1.4, there may be functions identified that are lower in level than the actual list of top-level functions to be associated with the current iteration of the process. Figure 4.4-15 is an example of a functional hierarchy using the list of identified autopilot functions.

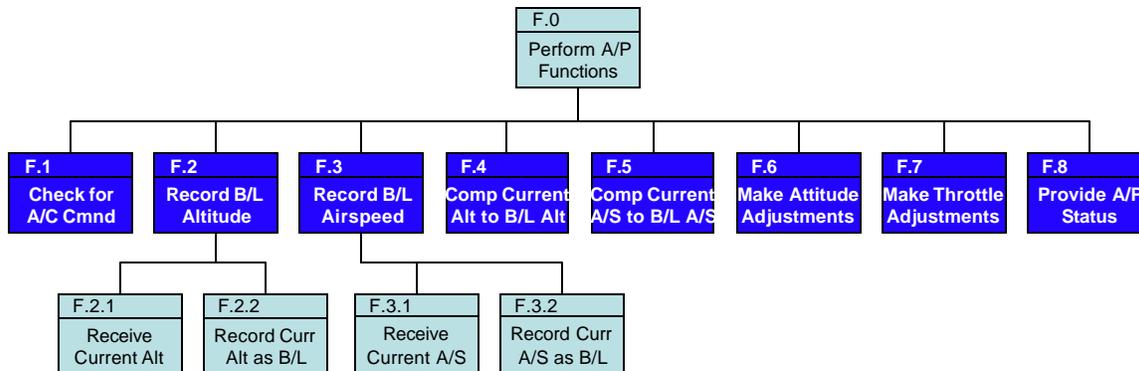


Figure 4.4-15. Autopilot Example Functional Hierarchy

Creating a hierarchy of all the identified functions ensures that the lower level functions are documented for later analysis. In Task 2, only the top-level functions will be considered (e.g., functions 1 through 8 from the list above rather than functions 2.1, 2.2, 3.1, and 3.2). A follow-on iteration of the process will handle the lower level functions

### Task 1.6 Create a Lexicon

In creating a lexicon, one defines the functions and data elements identified as providing the required system capabilities. It is recommended that these lexicon entries be defined with an eye toward converting the functional architecture into requirements and requirements into a physical architecture. Developing complementary functional and physical architectures requires multiple iterations between Functional Analysis, Requirements Management (Section 4.3), and Synthesis (Section 4.5).

The lexicon for a given Functional Analysis shall contain at a minimum the following information about a specific term:

- **Name** — either of the following: function name, data element name, or name of the data trigger
- **Type** — a function, data element, or trigger
- **Definition** — a detailed description of the term, including the full scope of its meaning
- **Unique Identifier** — a decimal delimited numeric identifier that facilitates insight into the model's functional hierarchy and data hierarchy (Figure 4.4-15 provides an example of a functional hierarchy, and Figure 4.4-16 provides an example of a data hierarchy.)
- **Source** — the originating source (document, person, organization) that facilitates future validation of any requirements associated with the term

D.1 Autopilot Status  
D.1.1 Engaged  
D.1.2 Disengaged  
D.1.3 BIT Error  
D.1.3.1 Altitude Hold Error  
D.1.3.2 Attitude Hold Error  
D.1.3.3 Velocity Hold Error

**Figure 4.4-16. Data Hierarchy Example**

The lower level working groups are responsible for coordinating their efforts with higher level working groups to de-conflict on the naming of terms. Thus, lower level Functional Analysis lexicons become subsets of any higher level lexicon.

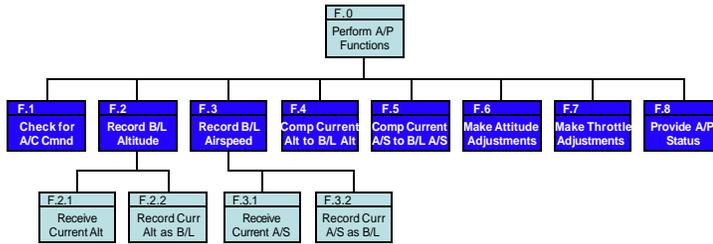
Affirmative answers to the following questions signify completion of Task 1:

- Has the problem space been clearly identified, including all missions, phases, modes of operation, and interfaces to and from the environment and other systems?
- Are assumptions documented with a plan of action to validate?
- Are all stakeholders identified and listed?
- Has a functional hierarchy been developed to organize the functions identified so far?
- Have all functional elements been properly identified and defined?

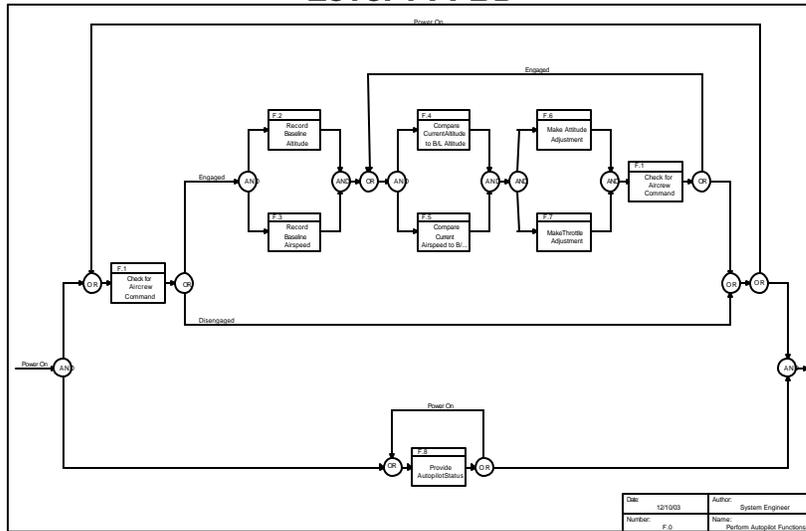
#### **4.4.4.2. Task 2: Organize Functions Into Logical Relationships**

The function list developed in Task 1 serves as an input to Task 2. This list includes the central functions required for the system to accomplish its mission; but the list functions are not necessarily arranged in a sequence or logical relationship. During Task 2, the highest level functions associated with this iteration of the process (i.e., functions 1 through 8 from the autopilot functional hierarchy) are logically arranged using an FFBD and an N<sup>2</sup> diagram (see **Figure 4.4-17**). The arrangement includes independent functions in parallel and dependent functions in series (e.g., when completion of the upstream function is necessary in order to begin the downstream function). Other diagramming techniques are to be used only when tailoring has been approved (subsection 4.4.6).

### Functional Hierarchy



### Level 1 FFBD



### Level 1 N<sup>2</sup> Diagram

Disengage Signal	Current Altitude	Current Airspeed	Current Altitude	Current Airspeed	Current Altitude			
Engage Signal								
F.1								Engage - Disengage Status
Check for Aircrew Command								
F.2	Record Baseline Altitude		Baseline Altitude					
F.3	Record Baseline Airspeed		Baseline Airspeed					
F.4			Compare Current Altitude to B/L Altitude		Altitude Delta	Altitude Delta		
F.5			Compare Current Airspeed to B/L Airspeed		Airspeed Delta	Airspeed Delta		
F.6					Make Attitude Adjustment			Attitude Adjustments
F.7					Make Throttle Adjustment			Throttle Adjustments
F.8					Provide Autopilot Status			Autopilot Status

Figure 4.4-17. Logical Arrangement of Highest Level Functions

The following subtasks are detailed and standardized steps to accomplish this second task using the FAA's preferred diagramming techniques.

#### Task 2.1 Document Assumptions

Document assumptions and issues where input is lacking (see Appendix D) and validate the assumptions with stakeholders as soon as possible.

#### Task 2.2 Create an FFBD

Create an FFBD (see subsection 4.4.3.1) for the highest level functions currently being worked (iteration dependent) from the functional hierarchy created in Task 1.5. Note that, alternatively, the N<sup>2</sup> diagram could be created first (see Task 2.3).



In this task, the highest level functions being worked in this iteration of the process are organized into their logical order of flow. Among the questions to ask to determine the logical order of flow are:

- Which functions depend on completion of other functions?
- Which functions depend on data from another function in order to begin execution?
- Which functions could execute in parallel?

Among the rules to remember when creating an FFBD are:

- For a function to begin execution, the preceding function or functions within the “control” flow must have completed execution. For example, in Figure 4.4-18, F.6 and F.7 can only begin execution once F.4 and F.5 have completed execution.
- For a function to begin execution, it may also need to be triggered with the input of data. For example, in Figure 4.4-18, before F.2 can begin execution, it will need “Current Altitude” data as well as F.1 to complete execution. Such data is referred to as a “trigger” and is captured in the N<sup>2</sup> diagram.

Figure 4.4-18 is an example of an FFBD using the level 1 autopilot functions.

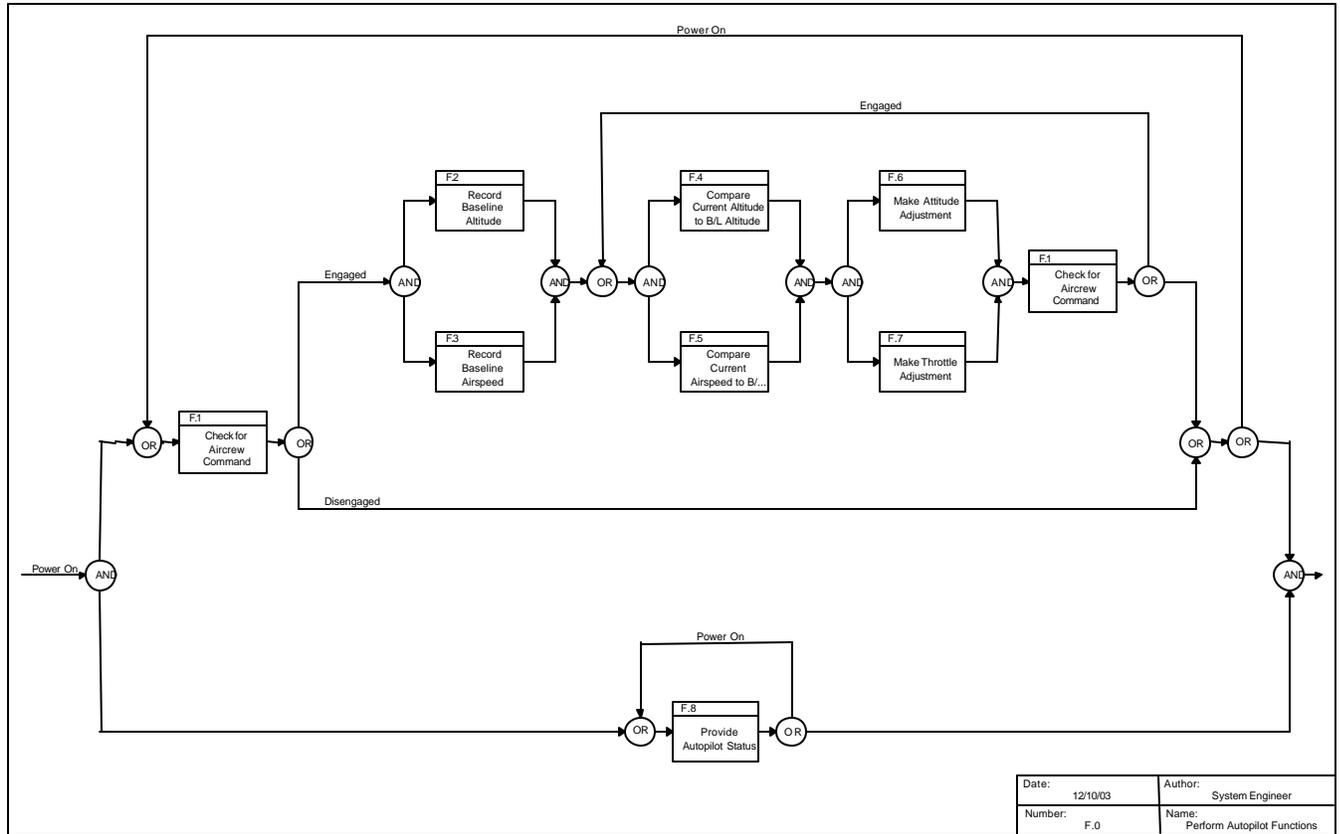


Figure 4.4-18. Autopilot Example FFBD

Task 2.3 Create an N<sup>2</sup> Diagram

Create an N<sup>2</sup> diagram (see 4.4.3.2) using the highest level functions currently being worked (iteration dependent) from the functional hierarchy.



Among the rules to remember when creating an N<sup>2</sup> diagram are:

- Compare a pair of the functions to determine the data that needs to be exchanged. For example, does F.1 produce any data that F.2 needs? If so, document the data to be exchanged in the appropriate cell. If not, leave the cell blank. Does F.1 produce any data that F.3 needs? And so on.
- Annotate the data items that are “triggers” required for parallel functions to begin execution (use color, or a symbol, or the letter “t”). For example, F.2 in Figure 4.4-19 needs “Current Altitude” data before beginning execution.

Figure 4.4-19 is an example of an N<sup>2</sup> diagram using the level 1 autopilot functions.

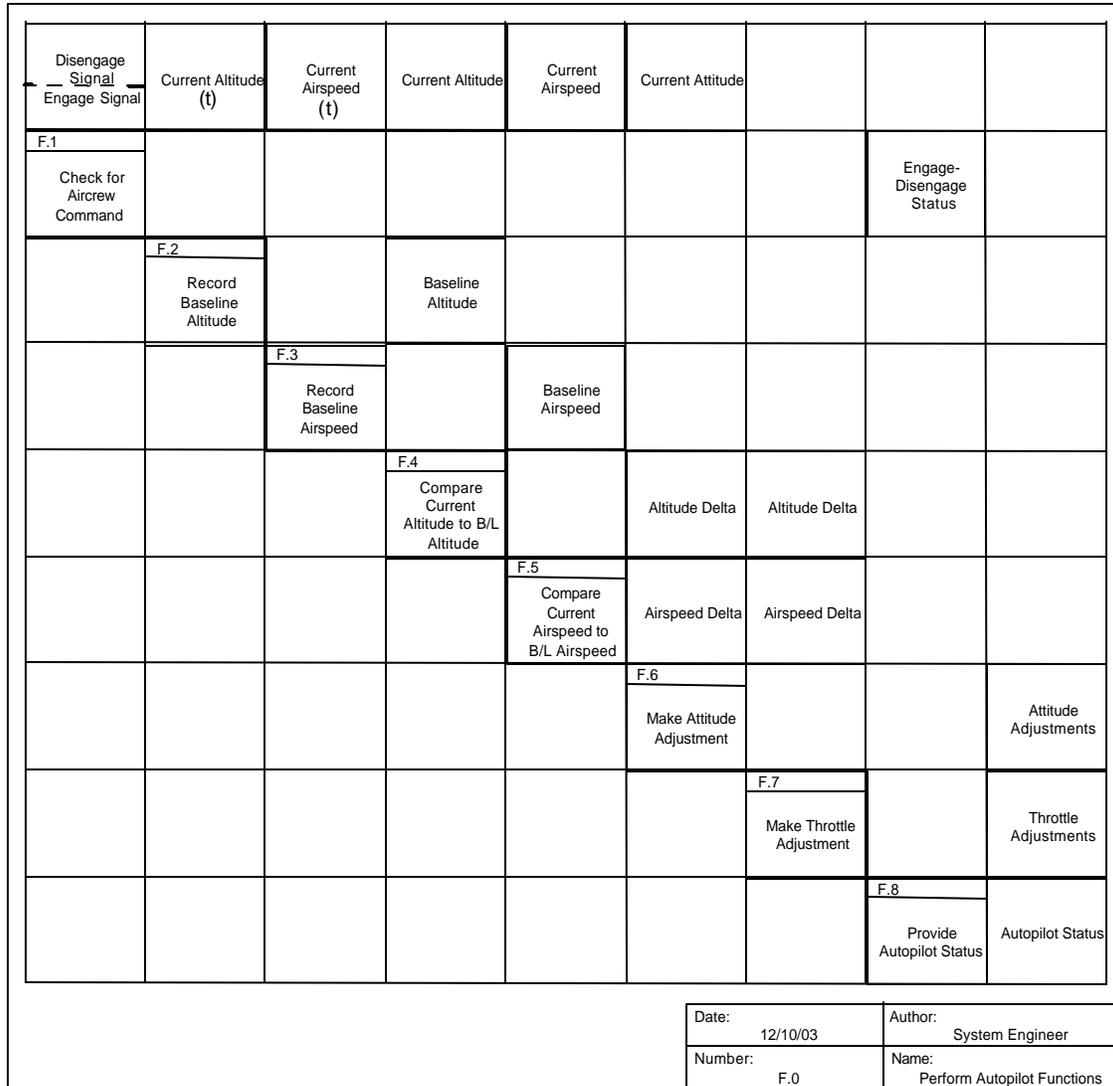


Figure 4.4-19. Autopilot Example N<sup>2</sup> Diagram

Task 2.4 Assign Decimal Delimited Numbers

This task involves assigning a unique decimal delimited number to each function, such as depicted below. Update all diagrams to depict the functions with their assigned decimal delimited number. This numbering system provides context regarding the location of a particular function in the hierarchy.

- F.0 Perform autopilot functions (the highest level function)
  - F.1 Check for aircrew command (level 1 function)
    - F.2 Record baseline altitude (level 1 function)
      - F.2.1 Receive current altitude (level 2 function)
      - F.2.2 Record current altitude as baseline (level 2 function)
  - F.3 Record baseline airspeed (level 1 function)
    - F.3.1 Receive current airspeed (level 2 function)
    - F.3.2 Record current airspeed as baseline (level 2 function)
- F.4 Compare current altitude to baseline altitude (level 1 function)

F.5 Compare current airspeed to baseline Airspeed (level 1 function)

F.6 Make attitude adjustment (level 1 function)

F.7 Make throttle adjustment (level 1 function)

F.8 Provide autopilot status (level 1 function)

#### Task 2.5 Define Data Flow Items

Define data flow items in the lexicon (see Task 1.6). The lower level working group is responsible for coordinating their efforts with the higher level working group in order to de-conflict on the naming of terms.

#### Task 2.6 Perform Peer Review With Identified Stakeholders

The newly created FFBD and N<sup>2</sup> diagram, along with the lexicon and any assumptions made, need to be peer reviewed with identified stakeholders. Based on the peer review, the FFBD and N<sup>2</sup> diagram should be modified as necessary.

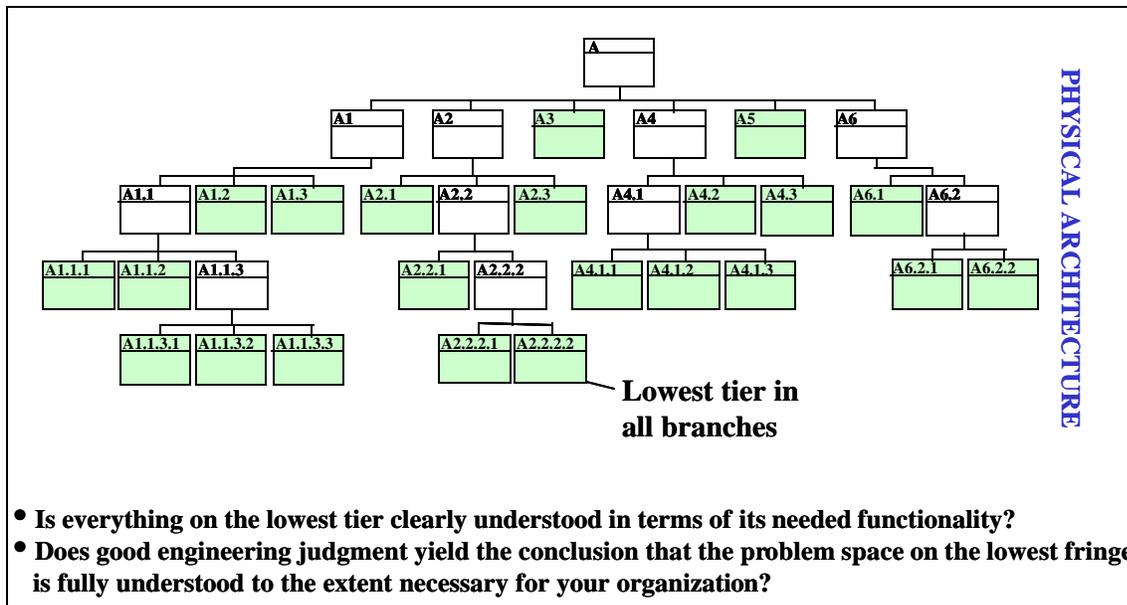
Task 2 is complete when yes is the answer to the following questions:

- Are all functions in the function list depicted?
- Are all functions written in the verb–noun format?
- Are all functional interfaces depicted graphically?
- Does the depiction show end-to-end functional relationships?
- Are parallel and serial relationships accurately depicted?

At this point, the results of the Functional Analysis effort should start to feed the Requirements Management process (see Section 4.3). The Functional Analysis effort can continue concurrently with requirements analysis tasks. However, since higher level requirements constrain lower level Functional Analysis work, the Functional Analysis effort should not get too far ahead of the requirements effort so as to avoid possible rework.

#### **4.4.4.3. Task 3: Decompose Higher Level Functions Into Lower Level Functions**

In this task, higher level functions are decomposed into subfunctions, with specificity increasing at each level of decomposition. Functional decomposition is performed using the techniques described in Tasks 1 and 2 regarding sequence and logical diagramming. The stepwise decomposition of a system basically is a top-down approach to problem-solving. Figure 4.4-21 through Figure 4.4-25 graphically show the execution of decomposition to a level at which the functions have been totally decomposed into basic subfunctions, and each subfunction at the lowest level is defined by its related valid requirement(s). This means that functional decomposition continues as long as there is need to define lower level requirements. When the requirements development process ends, Functional Analysis may cease. Completion of the requirements development process is based on developing the physical architecture. If everything on the lowest tier of all branches of the physical architecture (see Figure 4.4-20) is clearly understood in terms of its needed functionality, then development of the requirements can be completed. Ultimately, good engineering judgment is required to determine whether or not the problem space on the lowest fringe of the physical architecture is fully understood to the extent that a procurement specification or in-house requirements document can be completed from the performance and interface requirements perspective.



**Figure 4.4-20. End of Functional Decomposition**

The objective of Task 3 is to develop a hierarchy of Functional Analysis diagrams that describes the functions at all levels of the system. This hierarchy is only a portion of the functional architecture, which is not complete until all requirements and other constraints have been appropriately decomposed.

Task 3 is performed iteratively using the steps and techniques described in Tasks 1 and 2. Since higher level functions exist for this task, the subfunctions are based on the higher level functions developed in the previous tasks. In Figure 4.4-21, function F3 is decomposed into subfunctions labeled as the second level. Next, the functions in the second level are decomposed to the third level. This process continues until all the functions are totally decomposed into basic subfunctions, and each subfunction at the lowest level is completely, simply, and uniquely defined by its requirements. At each level, Functional Analysis feeds Requirements Management (Section 4.3), which feeds Synthesis (Section 4.5), as shown in and further illustrated in Figure 4.4-23 through Figure 4.4-25.

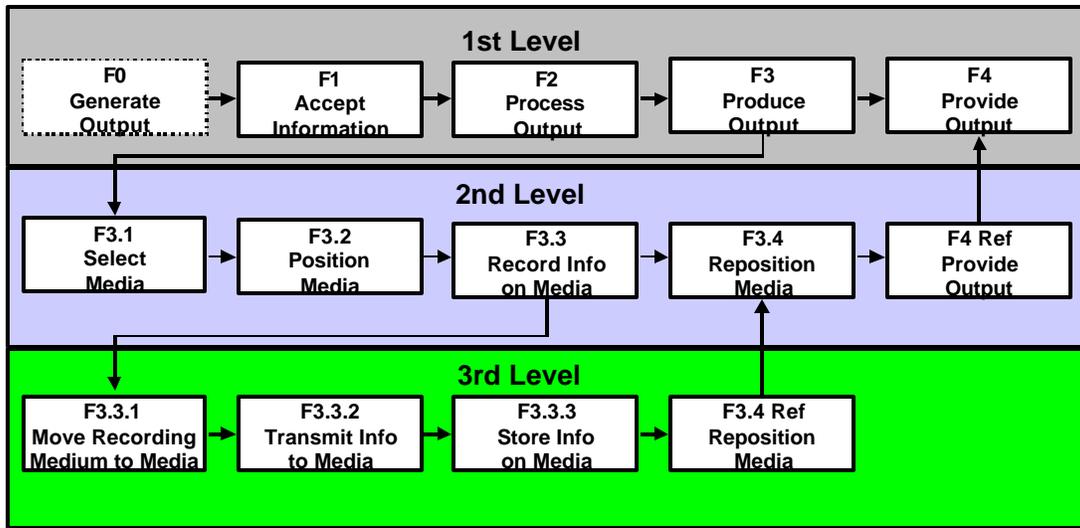


Figure 4.4-21. Breakdown of Higher Level Functions Into Lower Level Subfunctions

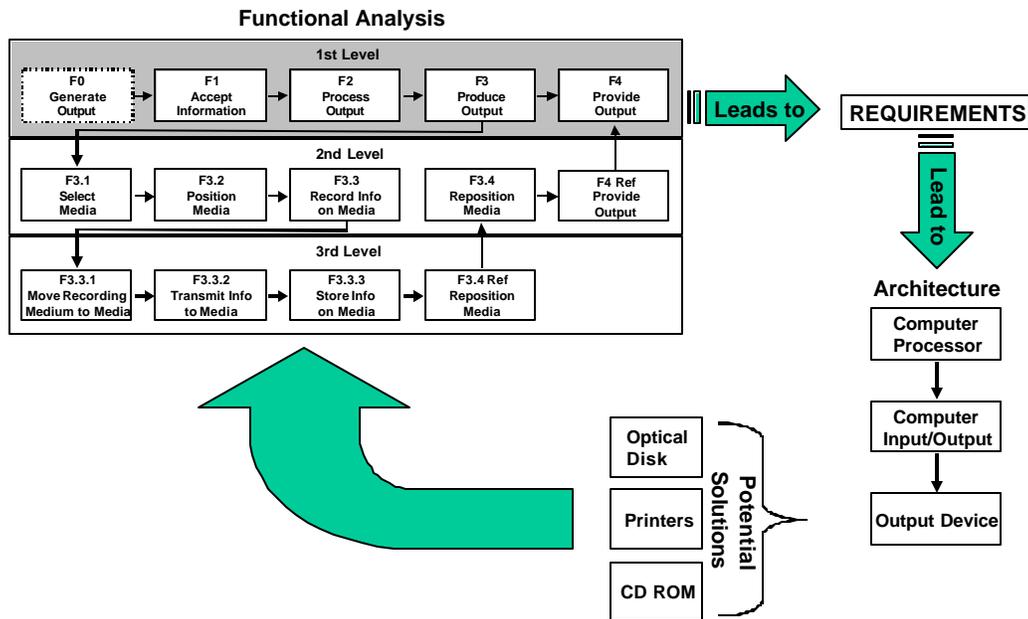


Figure 4.4-22. Functions to Requirements and Requirements to Physical Architectures

Requirements Management and Synthesis detail the process that turns functions into requirements and requirements into a physical architecture. It is important to note that the next Functional Analysis level is bound and framed by the requirements and physical architecture refined from the preceding Requirements Management and Synthesis activities.

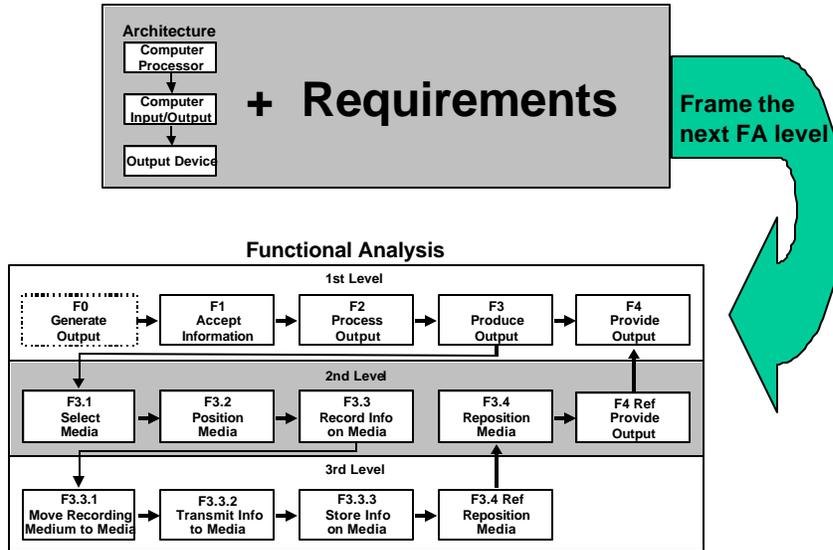


Figure 4.4-23. Requirements and Physical Architecture to the Next Functional Architecture Level

When this process completes one rotation, the Functional Analysis process restarts (see Figure 4.4-23 and Figure 4.4-24) at the next lower level. The process then repeats until each function is totally decomposed into its basic subfunctions, and each subfunction at the lowest level is completely, simply, and uniquely defined by its requirements.

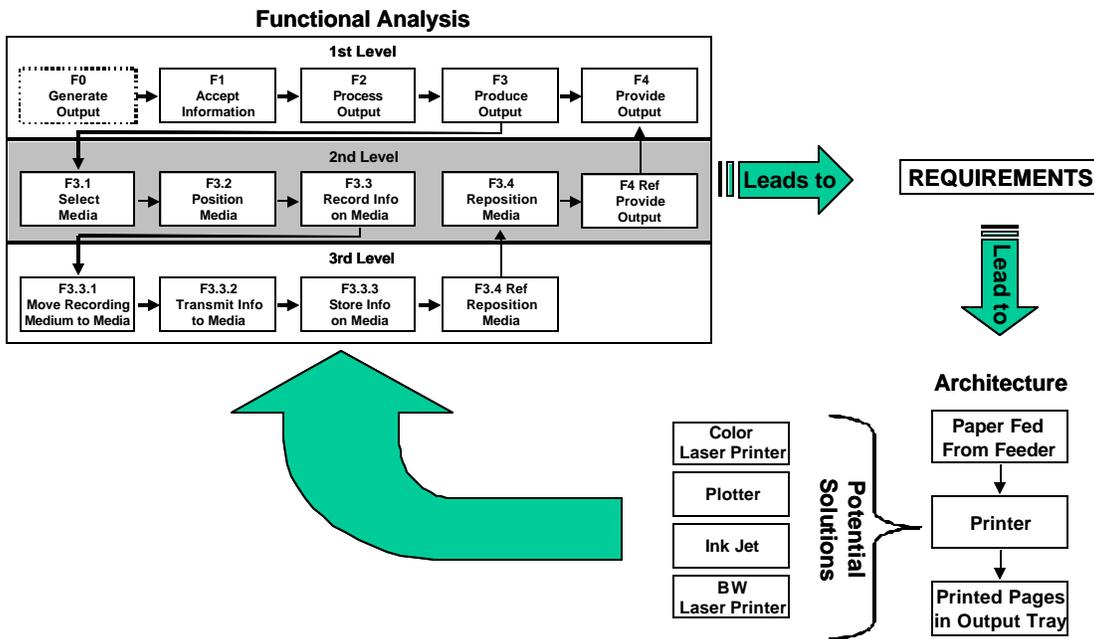


Figure 4.4-24. Repetition of the Functional Analysis Process at Next Lower Level

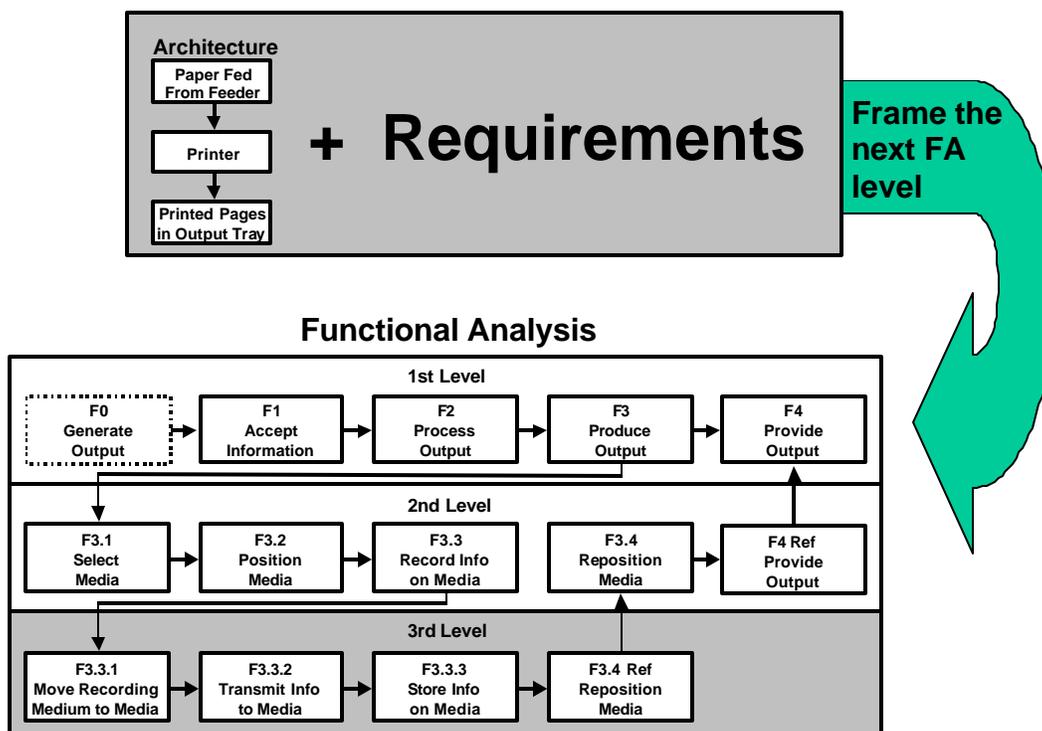


Figure 4.4-25. Preceding Requirements and Physical Architectures

Task 3 is complete when yes is the answer to the following questions:

- Has a complete set of Functional Analysis diagrams been prepared?
- Has each function been decomposed to its lowest level within program needs?
- Is each function completely, simply, and uniquely defined by its requirements?
- Has a description of each function been developed?
- Is the requirements development complete?

#### 4.4.4.4. Task 4: Evaluate Alternative Decompositions

This task evaluates alternative decompositions of functions (functional architectures) and requirements at all levels. These evaluations are necessary because there is no single “correct” decomposition; however, not all decompositions are equal. It is necessary to evaluate alternative decompositions to select the one best suited to the requirements. There are also other reasons to evaluate alternative decompositions. For example, as a result of Synthesis there may surface design constraints such as the desire to use commercial-off-the-shelf (COTS) or non-developmental item (NDI) components. Multiple functional architectures may then be produced to accommodate alternatives in accordance with various combinations of constraints. These are then compared using the Trade Studies process (Section 4.6) with the design criteria from Synthesis in order to select the functional architecture that most effectively meets mission objectives.

The evaluation of alternative decompositions of functions is subjective and depends on personal preference. Task 4 ensures evaluation of other methods to conduct the decomposition. In this task, personal preference and consensus among the stakeholders are factors in selecting the best functional architecture. Any selected functional architecture shall reflect the system's functions; however, variances in the alternative functional architectures may provide a competitive edge to one or more of the alternatives.

By the end of this evaluation process, the requirements for each subfunction at the lowest levels of the functional architecture are allocated via the Synthesis process to hardware, software, interfaces, operations, or a database, and then to a specific configuration item. (See Synthesis, Section 4.5, subsection 4.5.3.4, "Allocate to System Elements—Step 4.") Since it is necessary to verify requirements, the objective of Task 4 is to select those decompositions that promote straightforward requirements that may be validated and verified. (Validation and Verification (Section 4.12) further addresses this issue.) In addition, decompositions that enable a single function to be used at several places within the hierarchy may be identified, which simplifies development.

Task 4 requires "best engineering judgment," as the "goodness" of each functional decomposition is evaluated by measuring the degree that each module displays the following attributes:

- Performs a single function
- Is a logical task
- Leads to a requirement(s) that may be separately validated
- Has a single input point and a single output point
- Is independent within each level of the hierarchy (higher independence enables implementation of the module independent of the other modules)

One should consider using COTS or NDI hardware and software because a subfunction that has already been implemented in a compatible form on another system may be preferred to one that has not.

Task 4 is complete with selection of a final system functional decomposition.

#### 4.4.4.5. Task 5: Document Functional Analysis Baseline

The last task in the Functional Analysis process is documenting the results using a Functional Analysis Document (FAD). Figure 4.4-26 is an outline of the minimum items that the FAD should address. Section 5 and the appendices are the heart of what constitutes the functional architecture. The functional architecture shall be captured in the appropriate enterprise architecture (EA) view(s).

	Title Page
	Functional Analysis title
	Document version and date
	Signature block for approving authority
1	Introduction
	1.1 Purpose
	1.2 Scope
	1.3 Rationale
	1.4 Document Organization
2	References

3	Resources
3.1	Team Members
3.2	Stakeholders
3.3	Software Tools
4	Methodology
5	Analysis
5.1	Assumptions
5.2	Findings
	Appendix A — Context Diagrams
	Appendix B — Functional Hierarchy Diagram
	Appendix C — Functional Flow Block Diagrams
	Appendix D — N <sup>2</sup> Diagrams
	Appendix E — Lexicon
	Appendix F — Acronyms and Abbreviations

**Figure 4.4-26. Recommended FAD Outline**

Affirmative answers to the following questions signify completion of Task 5:

- Have all of the initial functions been decomposed into subfunctions?
- Do the subfunctions cover the total scope of the parent function?
- Are the functions arranged correctly regarding the dependence of the functions?
- Have all functional interfaces been defined?
- Have any new functional interfaces between initial functions been identified that were discovered during the functional decomposition process? (These may drive new system element interfaces.) If so, have the new interfaces been documented in control sheets?
- Has a Functional Analysis document been prepared to document the functional Baseline?
- Have all functional requirements been identified and decomposed?

#### **4.4.5. Outputs of Functional Analysis**

The outputs are static views of the results of the Functional Analysis tasks. As the FAA EA matures, these outputs will be migrated into the various EA views.

##### **4.4.5.1. Functional Architecture**

The most common output of the Functional Analysis process is a “living” functional architecture document that contains a tailored combination of the following:

- Functional architecture baseline
- Functional interface list
- Alternative decompositions
- Context diagrams
- FFBDs
- N<sup>2</sup> diagrams
- Other functional descriptions

#### 4.4.5.2. Concepts

In addition to the list above, documents capturing concepts related to the NAS may also be an output of the Functional Analysis process. The two types of concept documents are the CONOPS and the CONUSE. The CONOPS is a description of what is expected from the system, including its various modes of operation and time-critical parameters. The CONUSE is an extension of a higher level CONOPS with an emphasis on a particular NAS system<sup>1</sup> and its operating environment.

There are essentially three levels of concept documents—NAS-Level CONOPS, Service-Level CONOPS, and CONUSE—regarding system engineering the NAS. Figure 4.4-27 shows the documents' hierarchy.

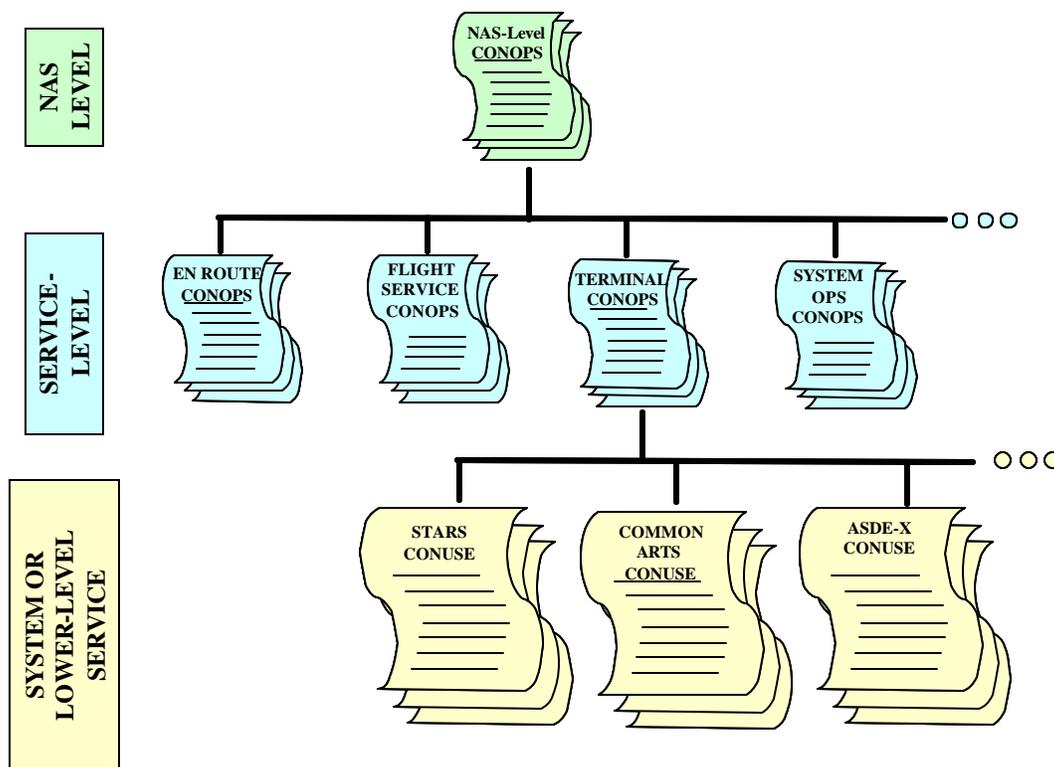


Figure 4.4-27. Concept Document Hierarchy

The NAS-Level CONOPS is a high-level narrative of the user community's desired change with some performance indicators. The document indicates from the user's perspective the desired end-state for respective systems in the NAS. It often uses various operational scenarios to illustrate the desired operational concept. These are characteristics<sup>2</sup> of a NAS-Level CONOPS:

- Describes the integrated operational environment (e.g., communications, navigation, and surveillance/air traffic management)
- Identifies current shortfalls and future needs

<sup>1</sup> Note that in this context and in concert with the SEM's definition of "system," this may be a lower level service rather than a physical system.

<sup>2</sup> These characteristics are adapted from an informal RTCA paper on CONOPS hierarchy.

- Provides a short-, mid-, and long-term perspective
- Identifies the functional requirements
- Identifies the approaches to address current deficiencies and future needs
- Identifies capabilities (without identifying specific technologies)

A Service-Level CONOPS provides conceptual insight into a particular service of the NAS. It gives more detail and in-depth information about the desired operations within the service (e.g., communications, surveillance, etc.). These are characteristics<sup>3</sup> of a Service-Level CONOPS:

- Describes a sub-element of the integrated operational environment
- Elaborates on the capabilities required for the specific service (e.g., communications, navigation, surveillance, etc.)
- Contains all the general categories from the high-level Operational Concept

A CONUSE is an extension of the NAS-Level CONOPS and a particular Service-Level CONOPS, with an emphasis on a particular NAS system<sup>4</sup> and its operating environment. It is more detailed and substantial, but it still expresses the user's needs regarding a specific system within the NAS. The CONUSE describes functional characteristics for a proposed system from the user's viewpoint; thus, it is essentially a system-level Functional Analysis narrative. It explains the existing system, current environment, users, interaction among users and the system, and organizational impacts. The CONUSE aims to communicate overall quantitative and qualitative system characteristics to the user, buyer, developer, and other organizational elements. The CONUSE aids in capturing requirements and communicating need to the developing organization. Posing the need in the user's language helps to ensure that the user can more accurately express the problem. Subsequently, the system engineers have a better foundation upon which to begin the lower level Functional Analyses, requirements definition, and initial system design. These are characteristics<sup>5</sup> of a CONUSE:

- Written in the user's language in the user's preferred format
- Written as a narrative (in contrast to a technical requirements specification)
- Tells a story using visual forms (diagrams, illustrations, and graphs) and storyboards whenever possible
- Links the user's needs and the developer's technical requirements documents
- Describes the user's general system goals, mission, function, and components
- Evokes the user's views and expectations
- Provides an outlet for user preferences
- Provides a place to document vague and immeasurable requirements (i.e., the user is able to state his/her desire for a fast response or reliable operation); these desires are quantified during the process of developing the requirements specifications and during the flow down of requirements to the physical architecture

---

<sup>3</sup> Ibid.

<sup>4</sup> Note that in this context and in concert with the SEM's definition of "system," this may be a lower level service vice a physical system.

<sup>5</sup> These characteristics are adapted from an informal RTCA paper on CONOPS hierarchy.

Figure 4.4-28 depicts the relationship between the three levels of concept documents. Following are the essential elements of all concept documents:

- Description of the current system or situation
- Insight into the user's environment
- Description of the functions to be performed
- Description of the needs that motivate development of a new system or modification of an existing system
- Insight into the new requirements
- Opportunity for the developer to recommend alternative solutions
- Description of the operational features of the proposed system
- User's view of the requirements

As Figure 4.4-27 and Figure 4.4-28 show, there should be traceability through a common content from a lower level CONUSE to the high-level NAS CONOPS.

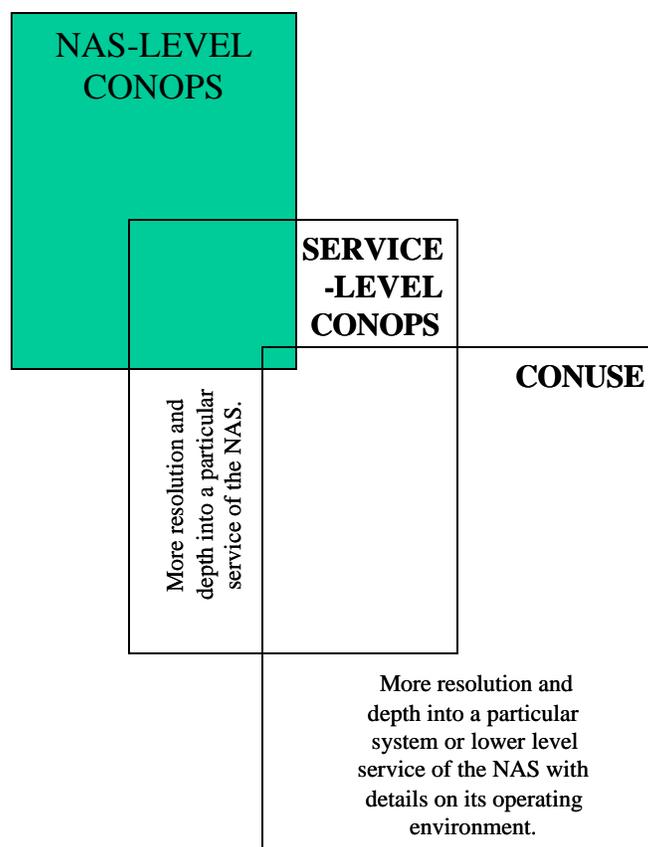


Figure 4.4-28. Concept Document Relationship

Figure 4.4-29 is a recommended outline for concept document content.

<b><u>CONCEPT DOCUMENT OUTLINE</u></b>	
1.	Introduction
1.1	Service or System Identification
1.2	Document Overview
1.3	Service or System Overview
1.4	References
2.	Operational Need
2.1	Current Service or System
2.2	Current Support Environment
2.3	Operational Problems
2.4	Objectives and Scope
2.5	Capability Shortfalls
2.6	Existing Operations Requiring Change
2.7	Constraints
2.8	Users
3.	Service or System Justification
3.1	Potential Benefit of New or Modified Service or System
3.2	Description of Desired Change
3.3	Change Priorities
3.4	Assumptions and Constraints
4.	Proposed Service or System
4.1	Objectives and Scope
4.2	Proposed Service or System Description
4.3	Proposed Support Environment
4.4	Modes of Operation
4.5	Users
4.6	Operational Policies and Constraints
5.	Operational Scenarios
6.	Impacts
6.1	Impact on Current Operations
6.2	Organizational Changes Required
	Appendix A. Glossary and Acronyms
	Appendix B. OSED (if available)

**Figure 4.4-29. Recommended Concept Document Outline**

The guide can be tailored to the document being developed and the information available. All three concept documents essentially contain the same information, but in varying degrees of detail. Thus, some elements in the guide may not be applicable due to the higher level nature of the information being published. The NAS-Level CONOPS is obviously broader in scope than a particular system's CONUSE; therefore, the depth of detail is less in a NAS-Level CONOPS. The breadth of a CONUSE is more focused and thus can contain more details.

#### **4.4.5.3. Planning Criteria**

Any planning criteria for performing Functional Analysis throughout the remainder of the program's lifecycle shall be provided to the Integrated Technical Planning process (Section 4.2).

#### 4.4.5.4. Operational Services and Environmental Description

The OSED is a comprehensive, holistic description of the services, environment, functions, and mechanizations that form a system's characteristics.

"What is a System?" A system (as defined in Chapter 2, subsection 2.2) 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.*

The 5M Model illustrated in Figure 4.4-30 represents this system view. Useful system descriptions exhibit two essential characteristics: correctness and completeness. Correctness means that the description accurately and unambiguously reflects the system attributes. Completeness means that all system attributes have been included and that the attributes are essential and appropriate to the level of detail called for in the description. System descriptions that include all 5M Model elements have these two characteristics.

The 5M Model states that there are five basic integrated elements in any system: (1) the functions that the system needs to perform; (2) the human operators and maintainers; (3) the equipment used in the system, composed of the hardware and software; (4) the procedures and policies that govern the system's behavior; and (5) the environment in which the system is operated and maintained.

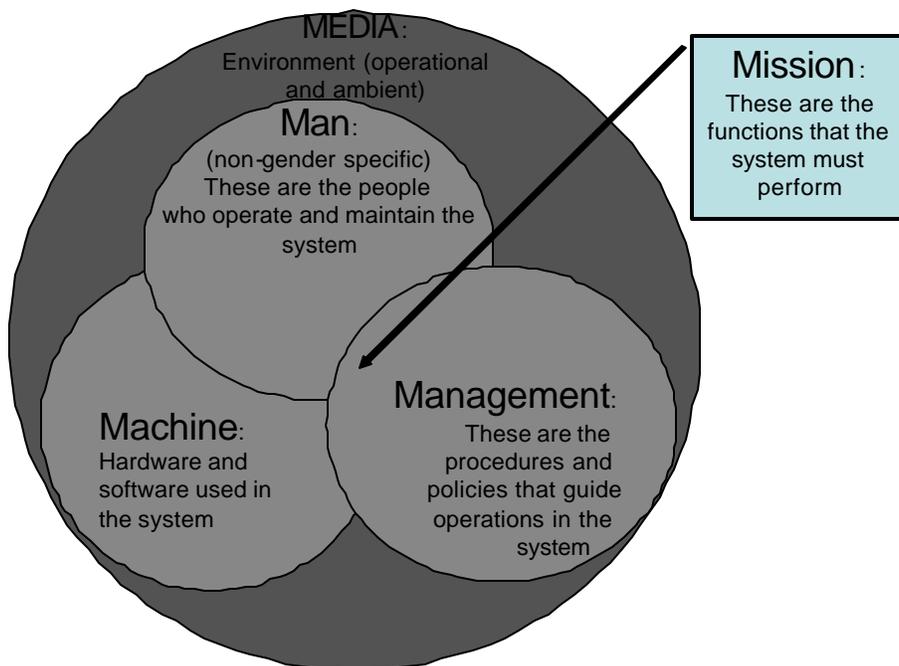


Figure 4.4-30. 5M Model

The document RTCA/DO-264, Annex C, contains detailed guidelines for the OSED for use as a starting point. These guidelines were tailored for the purposes of system engineering in the FAA. An OSED shall have, at minimum, the following information (Figure 4.4-31).

1. Operation Service Description: Summary of the air traffic services and operational context of the new capability from an operator's viewpoint.
2. Functional description or architecture: The functions and functional architecture in accordance with Functional Analysis.
3. Procedures: The existing and new procedures and policies that govern the system's operation or maintenance and includes:
  - a. Operational requirements and regulations, including separation minima
  - b. Deployment requirements
  - c. Operational scenarios
4. Human elements of the system: The operators and maintainers of the system, including information regarding:
  - a. Anthropometric requirements
  - b. Training requirements
  - c. Specific skill-set requirements
  - d. Human-system integration requirements
5. Equipment and software: Any known hardware and software that is required for system operation.
6. Environment description: An expression of the various conditions in which the system is operated, including:
  - a. Operational: factors such as traffic density and flow, flight phases, traffic complexity, route configuration, type of control, use of visual or instrument flight rules, etc.
  - b. Ambient: Refers to visual and instrument meteorological conditions, altitudes, terrain elevations, and physical conditions, such as electromagnetic environment effects, precipitation, icing, etc.
7. Nonfunctional requirements: Any other requirements that are not covered in the other sections and includes, but is not limited to, the following:
  - a. Time constraints
  - b. Information exchanges
  - c. Exception handling

Figure 4.4-31. Guidelines for an Operational Services and Environmental Description

#### 4.4.5.5. Constraints

Constraints on trade studies that surface as a result of performing Functional Analysis are to be provided to the Trade Studies process (Section 4.6).

#### 4.4.5.6. Concerns and Issues

Appendix D contains guidance on concerns and issues as a product of Functional Analysis.

#### 4.4.5.7. Tools/Analysis Requirements

Tools/analysis requirements for performing Functional Analysis throughout the remainder of the program's lifecycle need to be provided to the Integrity of Analyses process (Section 4.9).

#### 4.4.6. Functional Analysis Tools and Techniques

##### 4.4.6.1. Tools

Analysis tools may include but are not limited to general SE and design/simulation aids. Because requirements represent the basic thread through SE, Functional Analysis data shall be interoperable with requirements definition information. The results of the Functional Analysis process shall be captured in order to modify system requirements and other derived products.

Selection of a tool or tools shall ensure that the data is transportable and can be integrated with other related Functional Analysis results. A list of tools that may be used to perform Functional Analysis appears on the International Council on System Engineering Web site ([www.incose.org](http://www.incose.org)). The FAA's primary functional analysis tool is CORE.

##### 4.4.6.2. Techniques

There are a variety of other diagramming techniques besides FFBDs and N<sup>2</sup> diagrams, and system engineers, for professional development, should become familiar with them. The rationale for this is twofold: (1) There may be rare cases in which the preferred approach does not adequately address FAA needs, and thus the Functional Analysis process must be tailored, with justification and approval, to use an alternative technique to model the system's behavior; and (2) There may be cases in which contractors use different techniques to perform Functional Analysis, and the FAA engineers need to understand what the contractors mean. Among the various other diagramming techniques are:

- Network diagrams
- Time line sequence diagrams
- Hierarchical functional block diagramming
- Integrated Computer-Aided Manufacturing Definition (IDEF) diagrams
- Data/control flow diagrams and context diagrams
- State transition diagrams
- Unified Modeling Language (UML) diagrams



A good overview of various diagramming techniques and their merits appear in a paper, "Relationships between Common Graphical Representations in System Engineering," by Jim Long (available at [http://www.vitechcorp.com/infocenter/papers/CommonGraphicalRepresentations\\_2002.pdf](http://www.vitechcorp.com/infocenter/papers/CommonGraphicalRepresentations_2002.pdf)).

#### 4.4.7. Functional Analysis Process Metrics

Candidate metrics used to measure the overall process and products of Functional Analysis include the following:

- Percent of validated assumptions pertaining to the functional architecture
- Percent of identified functions incorporated into the functional architecture
- Percent of functions traceable to validated requirements
- Percent of functional elements clearly and completely defined in a lexicon
- Percent of data elements clearly and completely defined in a lexicon

- Percent of alternatives requiring further de-selection
- Percent of analysis studies completed (schedule/progress)
- Depth of the functional hierarchy as a percentage versus the target depth

#### 4.4.8. References

1. Blanchard, B. *System Engineering Management*. 2nd edition. New York, New York: John Wiley & Sons, Inc., 1997.
2. Blanchard, B., and Fabrycky, W. *Systems Engineering and Analysis*. 2nd edition. Englewood Cliffs, New Jersey: Prentice Hall, 1990.
3. *Certification Considerations for Highly-Integrated or Complex Aircraft Systems*. Aerospace Recommended Practice ARP-4754. Society of Automotive Engineers, 1996.
4. Defense Systems Management College. *Systems Engineering Fundamentals*. Fort Belvoir, VA: Defense Systems Management College Press, 1999.
5. *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. Aerospace Recommended Practice ARP-4761. Society of Automotive Engineers, 1996.
6. *Guidelines for the Approval of the Provisions and Use of Air Traffic Services Supported by Data Communications*. RTCA DO-264. RTCA, Inc., 2000
7. *Military Standard System Safety Program Requirements*. MIL-STD-88. Department of Defense, 1984.
8. NAS Modernization System Safety Management Program. Washington, DC: Federal Aviation Administration, 2001. (<http://fast.faa.gov/toolsets/index2.htm>)
9. *NASA System Engineering Handbook*. National Aeronautics and Space Administration, June 1995.
10. Sage, Andrew B., and Rouse, William B., eds. *Handbook of Systems Engineering and Management*. New York, New York: John Wiley & Sons, Inc., 1998.
11. *Systems Engineering Handbook*. Version 2.0. International Council on Systems Engineering, 2000.
12. Yourdon, Edward. *Modern Structured Analysis*. Englewood Cliffs, New Jersey: Prentice Hall, 1988.

## 4.5 Synthesis

**Synthesis is the creative process that translates requirements (performance, function, and interface) into alternative solutions resulting in a physical architecture for the “best value” design solution, consisting of people, products, and process solutions for the logical, functional grouping of the requirements.** In the Synthesis process, design engineers first conceive and then later refine specific designs that will serve to satisfy operational needs.

The Synthesis process defines design solutions and identifies systems that will satisfy the program requirements. Synthesis translates the requirements, as set in context by the functional architecture, into the design architecture, consisting of the physical architecture with its associated technical requirements. The resulting architecture provides an arrangement of system elements by designing their composition and interfaces, both internal and external. Additionally, the design architecture incorporates environmental, technical, and other constraints.

Synthesis is seldom, if ever, a one-step process, but rather accomplished many times over the life of a project in response to many factors. These include newly evolving technology, test data from the present or previous designs, changes in requirements from the user, changes in the price or availability of components, and feedback from the field once a system is deployed. As with all System Engineering (SE) functions, different objectives and activities exist within different phases of the acquisition process.

### 4.5.1 Introduction

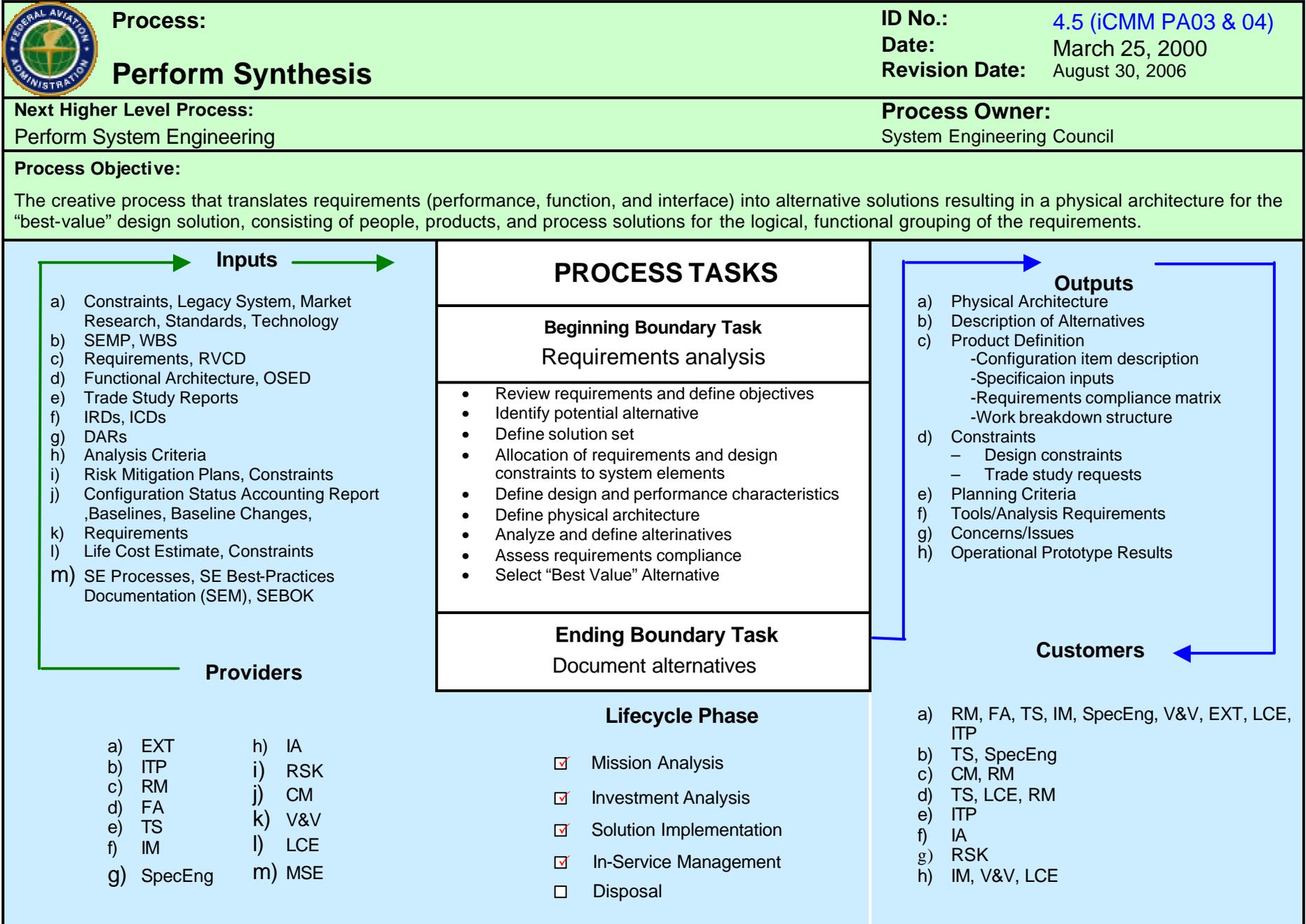
The Synthesis process is an element of the overall SE discipline, with other processes occurring before, during, and after. Synthesis also leverages the efforts conducted under various Specialty Engineering (Section 4.8) disciplines through concurrent engineering. Accordingly, Synthesis requires a number of inputs into the process in order to achieve the anticipated results, or outputs, of the process. See Figure 4.5-1.

Synthesis is conducted to translate the requirements (based on the functional architecture) into a physical architecture by defining and allocating the system elements. Those elements are then refined and integrated into the system's physical configuration, which satisfies the functional and performance requirements. This process relies heavily on prior establishment of clearly defined, documented, and validated requirements.

When entering the Synthesis process, do not assume that the entire requirements set associated with the functional area under consideration is achievable within the cost and schedule constraints. However, do assume that all requirements associated with the functional area under consideration have been validated in accordance with Validation and Verification (Section 4.12). The engineers involved in Synthesis work to find the best possible solution that will optimize achievement of the program requirements for the functional area under consideration. This requires close and continual coordination with Requirements Management (Section 4.3) and Functional Analysis (Section 4.4).

Success of the Synthesis or design process relies on a structured and disciplined approach to achieving the desired outcomes. The Synthesis outputs will naturally emerge from taking the appropriate steps during the design process. Conducted properly, Synthesis defines the build-to characteristics of the system or system elements. The Configuration Items (CI) are established and defined during Synthesis. At each level of the resulting design architecture, the requirements and interfaces must be verified. The Synthesis process must not only identify

technically feasible and programmatically achievable design alternatives, but the alternatives must also be well analyzed, documented, and finally placed under disciplined management.



**Figure 4.5-1. The Synthesis Process-Based Management Chart**  
4.5-3

### 4.5.2 Process Inputs

The Synthesis process starts at the conclusion of preceding key SE steps, as illustrated in Figure 4.5-2. These SE processes result in a number of outputs that will serve as necessary inputs to Synthesis.

Like Synthesis, the processes preceding it are not necessarily one-step processes. Each may undergo a number of iterations through the given process before the output is ready for the next process to begin. Additionally, the Requirements Management (Section 4.3) and Functional Analysis (Section 4.4) processes are tightly coupled, and a few iterations through these processes will occur before the outputs are ready to proceed into Synthesis.

Once it begins, Synthesis will be an iterative process, at times looping back through Requirements Management. This is known as the requirements verification loop. Synthesis might also at times initiate iteration back through Functional Analysis, known as the design loop. During these iterative loops through preceding processes, the program requirements and/or

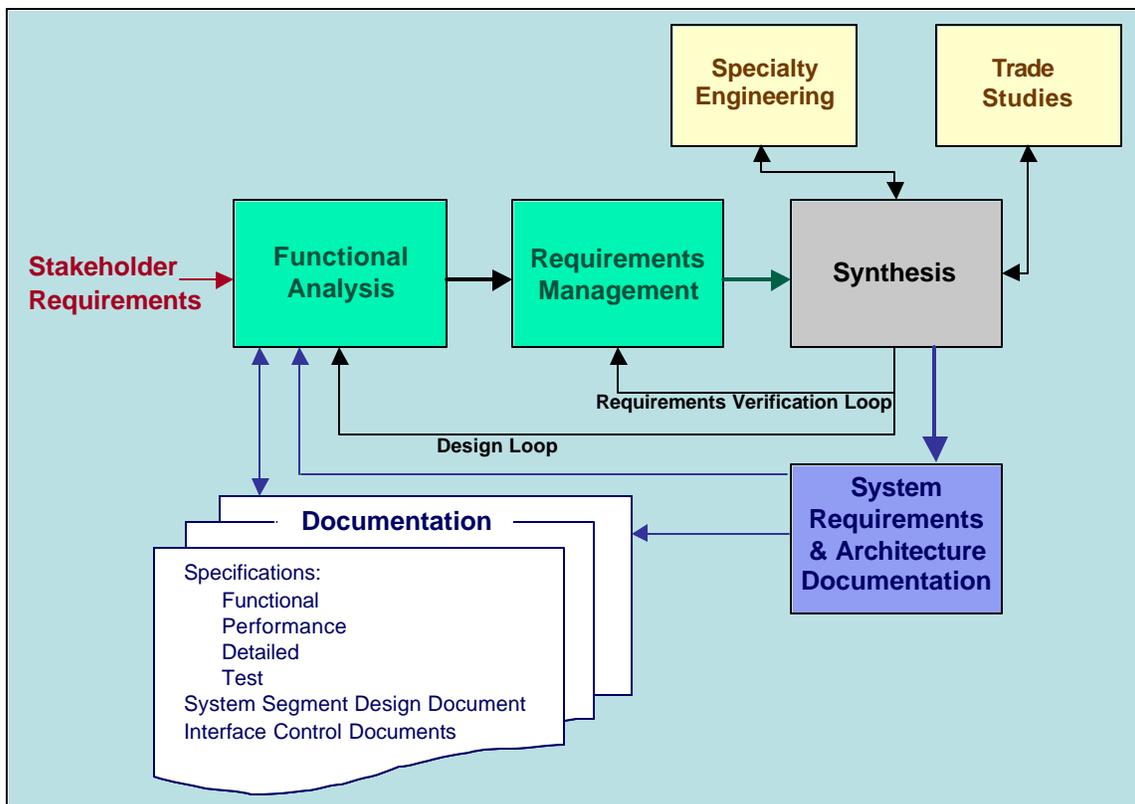


Figure 4.5-2: Requirements and Architecture Definition

functional architecture are constrained and refined to optimize the potential for viable design alternatives. This ensures that the functional architecture and requirements at lower levels of the physical architecture reflect the envisioned design.

#### 4.5.2.1 Initial Inputs

The inputs resulting from the previously conducted SE processes are known as the initial inputs because they serve to initiate Synthesis. They must be available before the start of system design.

#### 4.5.2.1.1 Functional Architecture

During Functional Analysis (Section 4.4), the high-level functions are decomposed to lower level functional groups or areas that can be satisfied by system design alternatives. The functional architecture must describe the functional arrangements and sequencing of subfunctions resulting from decomposition. The functional architecture does not consider design solutions, but only tasks or functions that the solution(s) must perform. Synthesis, by contrast, considers the grouped and decomposed functions, or functional areas, in light of technically feasible and achievable solutions.

Functional Analysis provides the design group the appropriate area of the functional architecture at which to begin the design process. This functional architecture is translated into an established requirements set that documents the problem or set of problems to be solved by Synthesis. The problem for the design group is to identify and define a system or systems that will adhere to the prescribed functional architecture while meeting stakeholder requirements.

#### 4.5.2.1.2 Program Requirements

The user needs and system functions are translated into a set of clearly defined, prioritized, measurable, and validated requirements (Section 4.3) for which the design group must provide a solution or solution set. The established program requirements (either preliminary Program Requirements (pPR) or final Program Requirements (fPR)), documented in the Exhibit 300 Attachment 1, dictate the tasks the system(s) under design must perform through functional requirements. The program requirements dictate how well the system(s) must perform its tasks through documented performance requirements. And finally, the program requirements ensure system compliance, function, and performance through measurable verification requirements on the Requirements Verification Compliance Document (RVCD).

Not only will information be needed regarding what the system must perform, how well it will be performed, and how performance will be measured, but the program requirements also establish the system's limitations. The program requirements contain the constraint requirements levied on potential solutions. Design 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. Acknowledged or not, the constraints determine the output of the system under design.

During the Synthesis process, the design engineers must consider the limitations of engineering. Often, "the laws of physics" or the "state of the art" limits solutions. The design engineers need to clearly understand technical as well as programmatic limitations to trade risk, schedule, and financial constraints in overcoming challenges to satisfying the program requirements.

#### 4.5.2.1.3 Legacy System Definitions

In the FAA, it is rare when a solution is introduced into a pristine environment (i.e., an environment where a system is not already satisfying user needs.) It is also rare that established needs do not evolve and change as the operational environment evolves and changes. Consequently, it is important to understand the existing legacy system that currently seeks to satisfy documented needs.

Understanding must include knowledge of the legacy system functions, performance, and its shortfalls. Only then can the design solution provide an alternative that improves existing capabilities, adds new functionality, and complies with evolving user needs. All documentation regarding system functional, performance, and constraint requirements is therefore a necessary input into the Synthesis process.

The design constraints imposed by the need for the system to operate with existing interfacing systems must also be understood. Interface Control Documents (ICD) will provide the information to ensure integration into the existing environment.

Finally, the new system must eventually operate in the existing support environment. Documentation regarding legacy system maintenance and support is needed to ensure that the system is designed in a manner that will enable it to continue to perform the needed user tasks at the needed level of performance once introduced into the support system.

#### **4.5.2.1.4 Implementation Strategy and Planning**

The Implementation Strategy and Planning (ISAP), the Exhibit 300 Attachment 3, is the document within the Acquisition Management System (AMS) that provides the strategy and planning for the detailed actions and activities necessary to execute the program within the cost, schedule, and performance constraints. The ISAP encompasses all elements of program implementation. This may include the acquisition of systems and equipment, construction or modification of facilities and the physical infrastructure, functional integration of planned capabilities within the existing infrastructure, and procurement of services.

To perform Synthesis, one must also know the schedule or budget constraints. If an ISAP exists, it provides this needed information. If such a plan does not exist, the design team will have to determine the cost and schedule constraints through interface with program management and other stakeholders.

#### **4.5.2.1.5 Operational Services and Environment Description (OSED)**

The OSED provides operational, safety, performance, and interoperability requirements. (See Functional Analysis (Section 4.4.5.4).) This document provides needed information for the Synthesis process. The OSED identifies the desired air traffic services and/or capabilities and their operational environments, including documented operational functions, performance expectations, and selected technologies. It defines the customer needs so that more appropriate alternative selections are considered during Synthesis.

#### **4.5.2.1.6 Preliminary Work Breakdown Structure (WBS)**

A preliminary WBS is provided and initially guides Synthesis efforts. (See Integrated Technical Planning (Section 4.2).) It is then refined under Synthesis by incorporating the characteristics necessary to support the functional and selected physical architecture(s) of potential design alternatives. The WBS defines categories of work, work packages, and, ultimately, through Synthesis, identifies associated physical elements. The WBS is invaluable from the planning and management perspective, since it establishes a top-down framework for allocating and computing costs. The WBS assists in tracking the status of engineering efforts, resource allocations, cost estimates, expenditures, and cost and technical performance.

During Synthesis, the WBS must be scrupulously maintained and finalized to show in a hierarchical manner all work elements needed to complete a given program or project. As solution physical architectures are defined, the physical elements are introduced into the WBS.

#### **4.5.2.2 Other Inputs**

Beyond the inputs available from SE processes occurring prior to Synthesis, there will be inputs gathered during Synthesis from sources both internal and external to the SE process.

##### **4.5.2.2.1 Market Research**

Market research is conducted during Synthesis to gather data to conduct the process as well as for various other reasons. During the phases of the AMS cycle, the role of market research in the Synthesis process will vary.

The first time through the Synthesis loop, when a pPR database has been established and provided as input to the Synthesis process, market research helps determine the available technologies 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 will be modified for optimization of alternative solutions. This optimization can occur numerous times as needed. During the final Synthesis iteration, the fPR is approved, and market research is conducted in concert with the design team to identify vendors that meet the finalized program requirements.

One final and important consideration for market research is to determine the market base for proposed design alternatives. A smaller potential market base for a system and/or its components will inevitably translate to an increase in cost risk and a greater potential for the market not to continue to produce the needed items for the needed timeframes as the demand for the supply diminishes. Market research is therefore valuable in determining not only what is available in the marketplace, but also in determining the extent of its availability and the likelihood that it will continue to be available for the required project/program lifecycle for which Synthesis will provide a solution.

#### **4.5.2.2.2 Risk Mitigation Plans**

Risk Mitigation Plans, although invaluable, may or may not be available for a given iteration through the Synthesis loop. For the initial time through the Synthesis loop, the fPR and functional architecture are not available. Therefore, the risks associated with potential design alternatives are undefined, and concerns and issues associated with those risks are not yet forwarded to the Risk Management process (Section 4.10) by the Synthesis team.

Subsequent iterations through the Synthesis loops, however, will have incorporated those initial concerns and issues, and a risk mitigation plan will have been developed under the Risk Management process (in concert with the Synthesis process).

#### **4.5.2.2.3 Trade Study Reports**

Trade Study reports are invaluable, whether available to the Synthesis process from previous related efforts or whether solicited through the course of the process. The Trade Study report provides documented answers to many issues and concerns for the Synthesis process, such as the feasibility of design alternative, the state of technology to support the alternative, and so on.

Existing Trade Study reports should identify related technologies that Synthesis may consider for incorporation into design alternatives. These reports provide valuable insight into what is feasible given the current state of the art.

When the Trade Study is conducted in concert with Synthesis, it is geared toward exploring and determining feasibility, associated risks, maturity of design, conformance to the program requirements and functional architecture, and adherence to the various constraints to the program/project. This input is solicited in the sense that the Synthesis process works in concert with the Trade Study process to determine objectives and needed outcomes for the Trade Study report. (See Trade Studies (Section 4.6).)

#### **4.5.2.3 Summary of Needed Input for Synthesis**

Availability of data depends on the status of the Synthesis process. If it is the first-time entry into Synthesis, or the first Synthesis loop, not all data will be available. However, as the Synthesis process continues, more data becomes available from other SE disciplines. Table 4.5-1 summarizes the data that is required and its availability for the Synthesis process.

Table 4.5-1. Needed Synthesis Data

Input	Delivering Process	SEM Reference	Availability
preliminary Program Requirements	Requirements Management	Section 4.3	First and subsequent loops
Functional Architecture	Functional Analysis	Section 4.4	First and subsequent loops
Legacy System Specifications	External to SE	N/A	First and subsequent loops
Legacy Interface Requirements	Identify, Define and Control Interfaces	Section 4.7	First and subsequent loops
Draft ISAP	Integrated Technical Planning	Section 4.2	First Synthesis loop
Operational Services and Environment Description	Functional Analysis	Section 4.4	First and subsequent loops
Preliminary WBS	Integrated Technical Planning	Section 4.2	First Synthesis loop
Market Research	External to SE	N/A	May not be available first loop through Synthesis
Trade Study Report	Trade Studies	Section 4.6	May not be available first loop through Synthesis
Risk Mitigation Plans	Risk Management	Section 4.10	May not be available first loop through Synthesis

### 4.5.3 Process Steps

Synthesis activities involve selecting a preferred solution or arrangement from a set of alternatives and understanding associated cost, schedule, performance, and risk implications. Synthesis entails undertaking a number of distinct steps to achieve measurable goals and objectives while striving to manage or overcome constraints. Alternative candidate designs are first conceptualized, and then candidate alternative solutions are defined and refined to meet the established program requirements.

Engineering analysis is used, as necessary, to evaluate alternatives. Evaluation will identify, assess, and quantify risks and select proper risk mitigation approaches. The risk management plan, if available, is used to refine the various design alternatives and achieve a balance between risk and technical progress. Too much risk within a given alternative could result in an unachievable design at the end. Assuming too little risk within a given alternative could also result in a solution that cannot be reached within the schedule constraints established for the project. These two extremes are balanced against the program requirements and established functional architecture through the guidance provided in the Risk Mitigation Plan(s). (See Integrated Technical Planning (Section 4.2)).

Analysis of alternative solutions also results in an understanding of cost, schedule, and performance impacts. As subsystem requirements are defined, identification of the needs, requirements, and constraints for lifecycle processes is completed. Figure 4.5-3 identifies the specific tasks that define Synthesis.

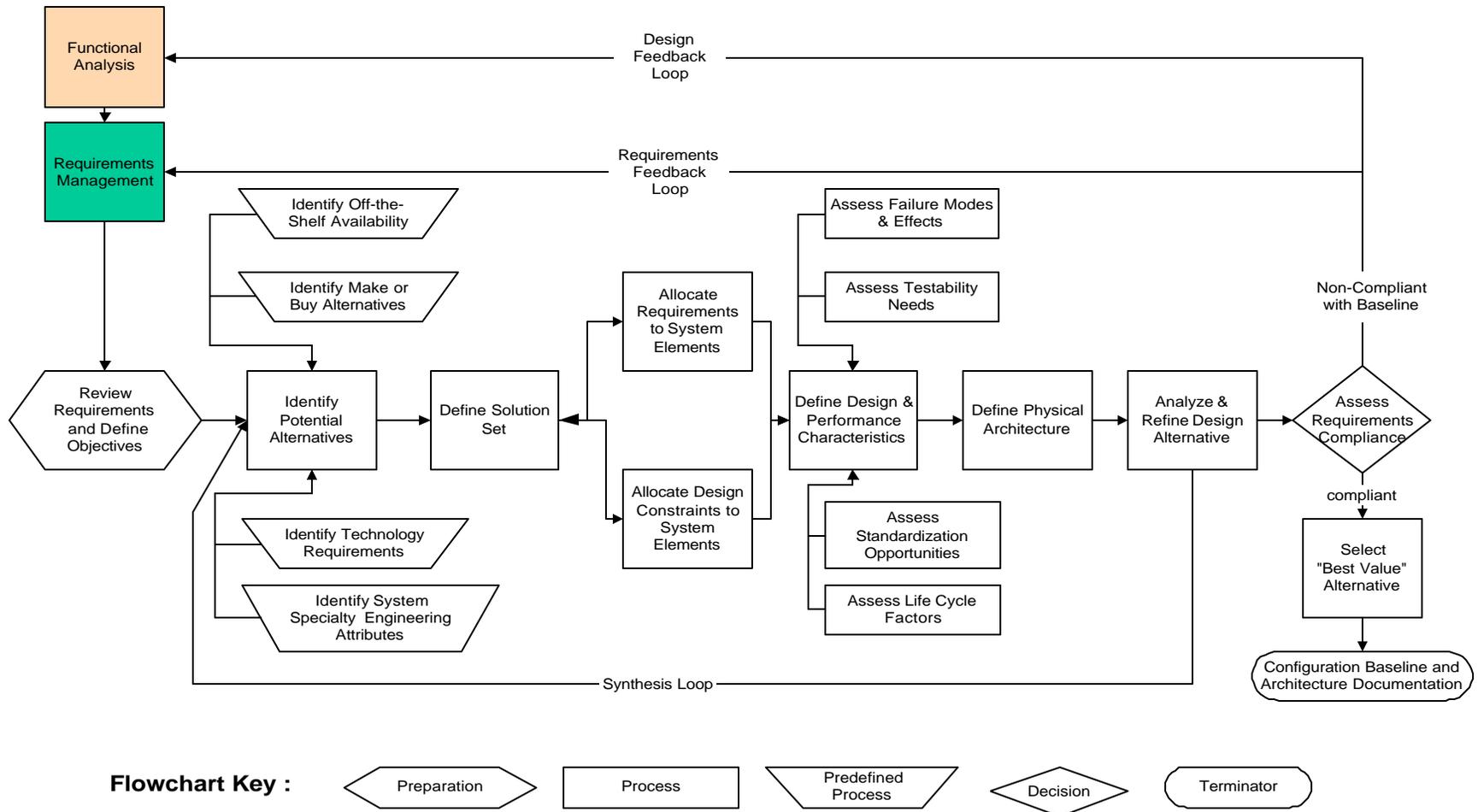


Figure 4.5-3: The Synthesis Process Activities

Synthesis demands creativity to achieve success. The ability to discover new solutions, to examine the requirements from new perspectives, and to formulate new concepts from two or more previously held ideas challenges the design group during this process. For the design team to succeed, each member must exercise awareness and sensitivity to problems associated with each proposed approach. Each person must exercise flexibility, originality, self-discipline, and persistence while maintaining adaptability, nonconformity, tolerance for ambiguity, self-confidence, and a healthy skepticism.

In addition to exercising individual characteristics, the team must also be aware of group characteristics and dynamics that are essential for successfully developing achievable yet satisfactory design alternatives.

A group of “*like-thinkers*” typically arrives at a mutually agreeable solution, or solution set, in less time and with less discourse than a diverse group with differing perspectives and priorities. The solution reached in this relatively pain-free manner will not have always considered and analyzed every facet of the approach and all problems associated with it. As a result, the solution may not in the end satisfy all the requirements and design constraints levied on the Synthesis process. The devil’s advocate plays an important role in the group and is as important to achieving the group’s goals as the consummate politician.

Once a diverse and well-balanced group is formed, the group, through various methods, can begin to develop design alternatives and a set of prioritized objectives. The group can use such methods as brainstorming, brainwriting, and dynamic confrontation (see text box at right). Whatever method or combination of methods is selected for this creative development of alternatives, the group should take care to ensure that no individual is allowed to dominate the group and, therefore, its outcomes. Likewise, the group must ensure that every member of the group has ample opportunity to contribute to the group’s efforts.

#### 4.5.3.1 Review Requirements and Define Objectives Definition—Step 1

After ensuring that all needed available Synthesis data has been gathered (see Table 4.5-1 above), 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

#### **Brainstorming**

*This technique involves both idea generation and idea reduction. First, idea generation occurs by simply identifying as many solution ideas as possible. Later, in idea reduction, those potential solutions are ranked into groups, with a specific group encompassing those potential solutions considered most useful to the group.*

*This technique is frequently considered a powerful one, as it often results in the most creative and effective solutions. These solutions may arise from a combination of seemingly unrelated ideas generated early in the process. Brainstorming encourages creative and original thinking.*

#### **Brainwriting**

*This technique builds on the concept of brainstorming, as it is the same technique but simply replaces verbal communication with writing. Using this technique, team members will write down a number of relevant ideas on a sheet of paper (usually limited to three ideas). The paper is then passed to another team member who then develops those ideas. New ideas and elements are added to the original concept(s) and the augmented pages are then passed to another team member.*

*This process continues until each team member receives back the sheet of paper containing the original concepts he/she created. At this point, the beginning phase is complete, and a group leader collects all idea/solution sheets.*

*The next phase begins with all sheets being handed out to the entire group. The group then works to revise the ideas developed in the prior phase.*

*This technique alleviates one of the problems associated with brainstorming: it prevents dominant members from easily steering the efforts of the entire group.*

#### **Dynamic confrontation**

*This technique is an adversarial group process. The main idea is for team members to criticize every idea. A presentation is first made and then every element and assumption of that idea is intensely challenged. This technique tests every idea thoroughly and forces all members to thoroughly think through and develop their ideas.*

meet stakeholder needs. Requirements Management will not dictate *how* the stakeholder needs will be met. The Synthesis process determines how to achieve stakeholder needs.

Establishing objectives assists in optimizing adherence to the requirements set within the technological and programmatic limits imposed on the design process. Objectives must be linked to stakeholder needs and system requirements. Objectives take into consideration, but are not limited to, operational criteria, mission success, technical performance, cost, schedule, quality, risk, failure rate, maintainability, and supportability. Through definition and prioritization of all design solution objectives, the optimal solution is achieved that best satisfies the requirements set under consideration.

Often, devices perform their functions at varying performance levels in differing environments. For instance, the system delay for a computer system gathering surveillance data from various sources and formulating a graphical representation of all existing air vehicles in a given space and presenting it to the controller on a display is vastly different at various locations and at various times during the day. Stakeholders would only state minimum National Airspace System (NAS) requirements for presentation of data to them from the source. The engineers involved in Synthesis must decide how they will meet those stated requirements in the various environments. A tailored system for each location might be provided, thus lowering the overall cost of upfront procurement, since computer systems with less processing power may be used in small airport areas. However, training and support regarding multiple systems must also be addressed in terms of added cost for multiple versions of the system. In this example, the Synthesis engineers must evaluate the operating environment of the solution to determine the performance objectives, upfront procurement cost, and the lifecycle costs of supporting the resulting system. These items represent three distinct objectives to be satisfied in selecting a design that will fulfill the stakeholder needs.

Another facet to consider is that a single system design may not necessarily satisfy all of the requirements associated with the functional area under consideration. Multiple systems may be required to satisfy the entire requirements set.

Ideally, alternative solutions should satisfy all requirements, but it is useful to include solutions that challenge the requirements and lead to a better system concept. Various options are to be considered eventually in light of the objectives for the resulting system(s). Such alternatives include relaxing requirements of marginal utility that are costly to implement or extending requirements when added capability can be purchased cheaply while accruing operational benefits.

#### **4.5.3.1.1 Performance Objectives**

The performance objectives, although highly dependent on potential system solutions, must be clear, as they serve to define the main purpose of the system. The engineering team must not only define all terms that will measure how the system will perform, but it must also state the actual desired performance levels. The team must review and analyze the accuracy, capacity, response time, throughput, and other similar requirements against feasible design possibilities. The threshold performance levels are clearly documented for the design under consideration. Most, if not all, of the performance requirements are contained in the program requirements provided under Requirements Management. However, the stated performance objectives that are to be achieved by any potential system or systems are clearly documented at the outset of Synthesis so that the tradeoff between these and other objectives may follow.

#### **4.5.3.1.2 Reliability Objectives**

The engineering team must define the reliability objectives in terms of the likelihood or probability that the resulting system will operate at its objective performance level for a defined period of time under normal operating conditions. In clearly defining these objectives, engineers

must translate the environmental and operational data, such as the data in the OSED. Allocation of the Reliability, Maintainability, and Availability (RMA) requirements in the program requirements is conducted in concert with the requirements process and Specialty Engineering in order to allocate the various reliability maintainability objectives to the various design alternative functional areas.

#### 4.5.3.1.3 Compatibility Objectives

The engineering team must define the objectives to enable the system to work or interface with both existing systems and those under agency development. Interface objectives are stated in terms of interfaces (including physical and functional descriptions (see Interface Management, Section 4.7, subsection 4.7.1.2)), but also in terms of the working environment imposed by the existing systems or system elements with which the potential design alternative must interact. The objectives must address both backward compatibility with legacy systems and forward compatibility with known evolving technologies, protocols, and standards.

#### 4.5.3.1.4 Flexibility Objectives

The engineering team must define the objectives to **enable alternative design approaches to adjust to a changing environment**. For example, the ability to process more flight data to adapt to a growth in air traffic must be clearly defined and documented. This is particularly important when it is known that the existing environment will evolve. The design alternative must evolve with the environment to adapt to the new environment. Projections for changes are documented along with the stated objectives for flexibility of the design alternative.

#### 4.5.3.1.5 Extensibility Objectives

Extensibility differs from flexibility, which means the ability to adapt to and accommodate growth needs. **Extensibility is the ability of the design alternative to serve new or multiple uses.** An example of extensibility is a multipurpose display that provides graphical display of flight plan data, surveillance data, or both simultaneously without need for modification.

#### 4.5.3.1.6 Cost Objectives

A limited budget is a never-ending facet of the Synthesis process. Thus, it is essential to define clearly the cost objectives at the outset for any potential design alternative. Try not to overemphasize cost of the item over all other objectives. The old adage, "You get what you pay for," is all too often true. Consequently, cost objectives are best stated within a range for the design alternatives. Cost objectives must include all facets of the potential design alternatives' lifecycle. Restricting objectives merely to the initial cost of a design solution may not fairly consider other design alternatives that have higher initial cost, but whose overall lifecycle costs are lower due to quality, reliability, and supportability characteristics. Therefore, the cost objectives shall be defined for all stages of the intended lifecycle.

#### 4.5.3.1.7 Schedule Objectives

What a design alternative will do, how well it will perform the function(s), and where it will perform become irrelevant if the design alternative is not delivered to the user when needed. A design alternative delivered too early is as potentially damaging to the effort as one delivered too late. Therefore, the schedule objectives for all facets of the design alternatives' lifecycle must be defined clearly and comprehensively. The schedule objectives for test, operational introduction, full operational capability, service life, and so on are all documented.

#### 4.5.3.1.8 Identify Objectives Tradeoffs and Define Objectives Hierarchy

Rarely, if ever, do projects have unlimited time and financial resources. Tradeoffs and compromises are common during Synthesis in order to achieve the design objectives with an

acceptable level of requirements compliance. It is essential to define the design objectives and rank their relative importance.

The prioritized set of objectives—defined during the brainstorming, brainwriting, and dynamic confrontation meetings—is to be well established and documented before design solutions are considered.

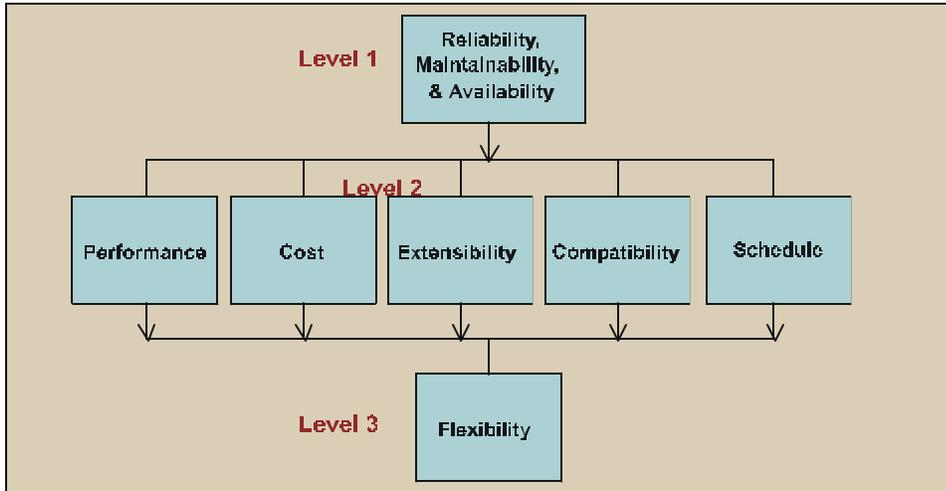


Figure 4.5-4. Example Three-Level Objectives Hierarchy

Objectives from the above categories and additional categories to be considered under the program/project are first documented as a list. The list is expanded to include more categories as determined necessary in concert with program management, Specialty Engineering, and stakeholders. The importance of each

objective relative to the others is then determined for all objectives. Once all the relative priorities are established, priority levels are defined based on the findings. This task, although not simple, is necessary because the results are invaluable later when design alternative tradeoff analysis is performed.

Assume that each of the categories of objectives just described has one objective; there are then a total of seven resulting objectives. For this example, examine a project that eliminates a reliability deficiency in an existing fielded system. In this particular example, RMA is therefore considered more important than all other alternatives. Also, since the product introduced is only an interim solution to fulfill a shortfall, system flexibility is considered less important than all other factors. If all remaining objectives are considered to be of equal importance, there are three priority levels (Figure 4.5-4)

Establishing the objectives hierarchy is seldom this simple. The items in level two of the figure are rarely seen as equal in importance. This level may be further broken down into groups, with each group containing objectives of equal importance and with one group being considered to be more important than the other. This

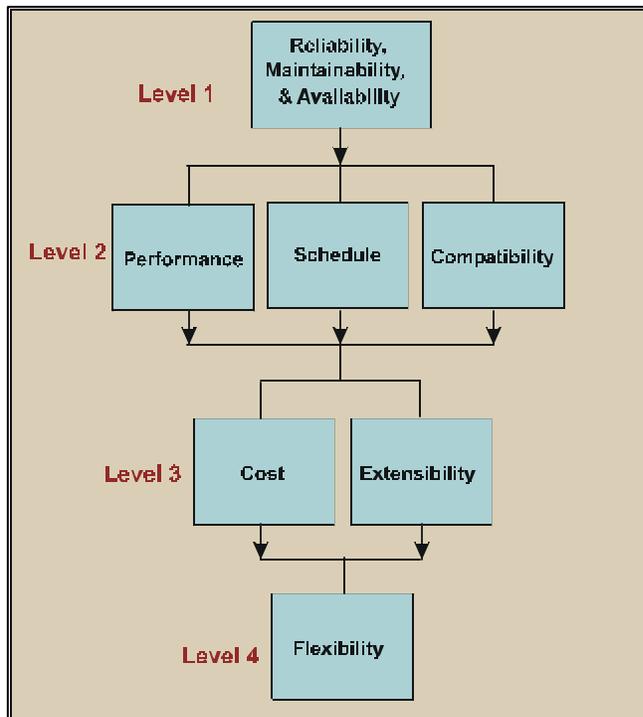


Figure 4.5-5. Example Four-Level Hierarchy

leaves four levels of priorities instead of three, and the hierarchy is established, with relative objective priorities and priority-level definition (Figure 4.5-5).

### 4.5.3.2 Identify Potential Design Alternatives—Step 2

During this step, grouping of needed functions into common functional areas is complete, and the functional architecture is established. The design team must now begin partitioning desired requirements into design elements. In reviewing various designs regarding whether or not they will perform the desired functions, the team maps each requirement, grouped functionally in the functional architecture, to a component of the system under review. Some components will satisfy one requirement, whereas others may satisfy more (Figure 4.5-6).

This Synthesis process step boils down to generating alternative design solutions for the functional elements identified during Functional Analysis (Section 4.4) that perform the needed functions and adhere to the requirements for that functional area. The alternative solutions should be composed of one or a combination of more than one of the following: hardware, software, material, data, facility, people, and techniques.

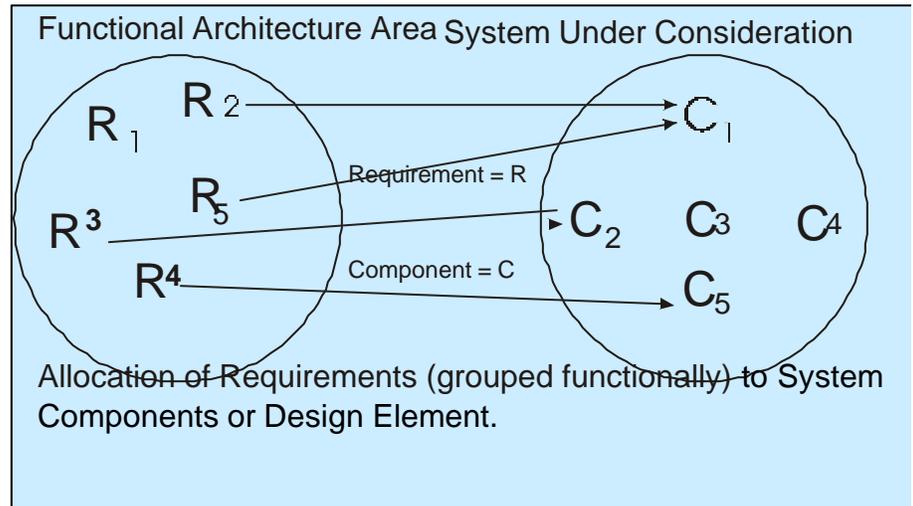


Figure 4.5-6. Functional Partitioning to System Components

There are a variety of tasks conducted to identify an array of design alternatives. Various subteams may perform the tasks sequentially or concurrently. If the Synthesis team is small, it is best for all members to consider identifying alternatives sequentially. If the team is large enough and good communications exist among all members, the team should explore concurrently identifying solutions by the various means described in the subsequent subsections. Both approaches require that the entire group conduct prior planning. Concurrent exploration of alternatives requires close coordination throughout identification of alternatives until all possibilities are identified; whereupon, the subteams will once again combine to complete this Synthesis step. Figure 4.5-3 (above) illustrates the tasks feeding the Synthesis step that identifies the various design alternatives.

#### 4.5.3.2.1 Identify Technology Requirements

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 being considered is analyzed against the changing technologies available in the marketplace. Available technologies are studied for use in the design under consideration, potential improvements to design performance, improvement to maintainability of the resulting system, cost-effectiveness, and maturity.

The need for a new technology that makes possible a performance or functional improvement previously not possible 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.

To continue consideration of the potential technology insertion, the impacts to the end user must be considered through human factors analysis. The tasks, roles, and jobs assigned to humans are analyzed and assessed to discover whether the end users of the resulting system have the required knowledge, skills, and abilities. If the knowledge, skills, and abilities do not exist, then the cost and schedule risks of achieving them with the new technology are weighed against the benefits derived from the technology. Training and personnel pipelines are fully evaluated to ensure that they meet requirements.

#### **4.5.3.2.2 Identify System Specialty Engineering Attributes**

The design team must work in concert with specialty engineers to identify the characteristics of each potential alternative necessary to fulfill interdisciplinary needs.

The design team and specialty engineers work together to:

- Analyze each alternative
- Identify potential hazards to system hardware/software components
- Identify the humans involved in the system as users or support personnel
- Identify characteristics of the proposed operational environment

The analysis must demonstrate that the design under consideration results in safe system operations. The analysis includes all aspects of the design, development, manufacture, test, operation, and support of the potential design.

The design team works with human engineering to analyze each alternative for human factors suitability. Each alternative is analyzed regarding the human user system interface. (See Specialty Engineering (Section 4.8).)

#### **4.5.3.2.2.1 System Safety Engineering**

System hazards are identified and assessed for the design alternative. The hardware, software, operational, and ambient environments, as well as procedures and human elements of the design alternative, are analyzed. Historical or test data is applied to estimate the risk (severity and likelihood) of each identified hazard. Controls are then designed in accordance with the safety order of precedence described in Specialty Engineering (Section 4.8) subsection 4.8.1. All hazards and their associated controls are prioritized according to their risk criticality rating. The analysis results are used to direct further design efforts to characterize controls, safety features, redundancy, and system degradation elements of the system.

#### **4.5.3.2.3 Identify Off-the-Shelf Opportunities**

Each design alternative is analyzed to determine if an off-the-shelf item exists that will fulfill the allocated requirements. Off-the-shelf solutions can include non-developmental hardware or software.

Once off-the-shelf solutions are identified, each must be assessed to ensure that a variety of factors are considered in determining suitability. The number of systems available off the shelf must be gauged against the number that users need. The quantity required must include not only those needed initially by the user community, but also those needed to serve as replacements over the anticipated service life of the system.

Another facet of the suitability assessment process is consideration of the environment in which the prospective off-the-shelf item must eventually operate. The proposed item must be able to adapt to the existing support structure to be suitable. If the item requires new equipment and/or training for support during its lifecycle, the benefits of the item must outweigh its cost and schedule impacts.

Finally, the manufacturer(s) of the off-the-shelf item must be assessed. Attributes such as product maturity, upward/downward compatibility, manufacturer track record, financial stability, and quality practices must be factored into the commercial product selection process. If the products or manufacturers fall short in any of the reviewed categories, they must be considered a risk. Refer to Appendix F of the FAA COTS Risk Mitigation Guide (at <http://www.faa.gov/aua/resources/cots/intro.htm>) for a more detailed listing of COTS nontechnical selection factors.

#### 4.5.3.2.4 Identify Make-or-Buy Alternatives

A cost analysis is performed for the design alternative(s) and used to support a make-or-buy decision. This analysis must address whether it is more cost-effective to produce the design element or use an established supplier.

When cost, schedule, and risk are considered, the best choice is to design and develop (a “make” decision) a singular system that satisfies all functional area requirements. The team will proceed with this approach as a viable design alternative.

#### 4.5.3.3 Define Solution Set—Step 3

Input from prior processes and previous Synthesis steps identify not only potential alternatives, but also design constraints for potential solutions. This input is used to help determine if existing or newly developed items can accomplish the function under consideration.

Synthesis strives to identify viable design alternatives, refine those alternatives to fulfill the program requirements, and finally select the most balanced and beneficial design to introduce into the field. To accomplish this goal, all possible alternatives are first identified. These are reduced to reflect only those alternatives considered viable or worth pursuing.

##### 4.5.3.3.1 Populate the Solution Set

The design team identifies all possible design solutions that may serve to satisfy all or part of the program requirements. After exploring and then exhausting these possibilities, team members, as a group and individually, evaluate the design solution set. If only one possible design alternative has been identified, then the job is not complete. No matter how large or difficult the program requirements and their associated functional area are, there will always be at least one possible design alternative: *do nothing*—that is, continue the status quo and not present new and/or innovative design solutions. Given the fact that a great effort went into previous SE processes (such as Requirements Management (Section 4.3) and Functional Analysis (Section 4.4)), it is unlikely that entrance into Synthesis would have occurred if all requirements in the functional area, with its associated program requirements, were satisfactorily met. Clearly, it is possible to identify an insufficient number of alternatives. The task is to develop additional alternatives that present better options.

The following methods can be used to develop new alternatives.

- **Change the characteristics of existing alternatives.** First, list all existing alternatives and then itemize the main characteristics of each. Generate a table with the rows representing the list of alternatives and the columns representing the main characteristics of all alternatives. In all likelihood, each of the potential alternatives will possess characteristics that are both similar and distinct from those of the other alternatives. Identify the positive characteristics and then list the missing characteristics needed by a design alternative and not represented by any potential solution. Finally, add more alternatives to the list, since the characteristics within the previously listed alternatives are varied. This addition enhances the new alternatives with needed positive characteristics and eliminates as many negative characteristics as possible.

- **Return to the objectives.** Focus on the most important objectives one at a time and list alternatives that will meet each of those top-level objectives. Then, work down the objectives hierarchy, developing more alternatives or refining existing alternatives that satisfy those additional objectives.
- **Finally, examine all the objectives and requirements set.** List alternatives that will maximize the number of objectives and requirements that can be met with the alternative.

If there still seems to be a lack of viable alternatives, step through the various methods, introducing more creativity and ingenuity each time through. Eventually, a solution set will reach a stable point, and identification of design alternatives is complete.

Having identified a significant number of design alternatives, one must now evaluate all alternatives. First, determine that a number of sound viable design alternatives exists that can satisfy all or most of the program requirements. It is possible to continue the Synthesis process with too many design alternatives because the remaining steps will detail and document each alternative to a great degree. Therefore, continuing with too many alternatives can waste valuable time and resources. One can argue that proceeding with one alternative is not sufficient. Likewise, one might also argue that proceeding with 10 alternatives that must be thoroughly defined and documented is unnecessarily excessive; so, reducing the alternatives set to a manageable size or number of alternatives (based on the scope of the stakeholder need) is a must.

#### 4.5.3.3.2 Reduce Solution Set to Manageable Number of Alternatives

When viable design solutions are identified, one must not compromise **requirements considered absolutely necessary to satisfy the operational needs. These requirements—which a system must meet or be deemed unnecessary or unacceptable—are to be considered “*threshold requirements.*”** A potential design solution must satisfy threshold requirements for further consideration as a design alternative. Threshold requirement compromise or tradeoff is not an option. A design alternative not meeting a threshold requirement that cannot be modified easily to meet the requirement(s) is eliminated and not considered further.

The objectives hierarchy is used next. If the remaining alternatives set contains potential solutions that do not meet the top-level objectives—and they cannot be easily or affordably modified to do so—then they are eliminated from the set of potential alternatives. As with requirements, some objectives are not subject to compromise, and alternatives not meeting the high-priority objectives, as defined earlier, should no longer be considered.

If potential solutions are only able to satisfy a portion of the functional area requirements or objectives, consider various options to develop a set of viable design solutions. One or more of the solutions that nearly satisfy the objectives and/or requirements could be modified to achieve satisfactory results. The following options may be used to modify either the problem (functional area under consideration with its associated requirements) or the alternative design solutions.

- **Request Trade Study.** A detailed analysis, such as that conducted under Trade Studies (Section 4.6) is requested to determine if one or more of the options can be modified to fulfill the desired requirements and/or objectives. Under the Trade Studies process, incorporation of new technologies and a variety of other means are investigated. If the results of the study render viable design alternatives, then Synthesis proceeds to the next step, requirements allocation. However, if no alternative can meet all of the requirements in the functional area under consideration, the requirements and/or the functional areas are analyzed.

- **Initiate Requirements Feedback.** When the program requirements for the functional area under consideration cannot be satisfied through viable design alternatives, feedback to Requirements Management (Section 4.3) is initiated. If program requirements are only partially met by all potential designs, Synthesis and Requirements Management concurrently analyze the ability of the alternative solution to meet the requirements set. Consideration is given to modifying requirements to lower and achievable levels. Full compliance is deferred until technological or other advances allow for full compliance with the original requirements. Requirements that cannot achieve even partial compliance in the various designs are addressed through the design loop.
- **Initiate Design Feedback.** Due to discovery of design issues, the Functional Analysis (Section 4.4) is reexamined, and the initial decomposition or performance allocations are reassessed. Design issues include identifying a promising physical solution or open-system opportunities that have different functional characteristics than those foreseen by the initial functional architecture requirements. Issues also include the inability of all design alternatives to fulfill the same functional architecture; this may be addressed by repartitioning the functional area. The functional area is subdivided so that allocation of those requirements to be satisfied by the alternative designs can be made down to perspective system elements. The remaining functional areas whose associated requirements will not be satisfied remain with the Functional Analysis (Section 4.4) process. The associated requirements are documented as unsatisfied in the Requirements Management (Section 4.3) process. The functional area(s) with the associated unsatisfied requirements are partitioned out of Synthesis back to Functional Analysis for future Synthesis loop identification of potential solution(s).

All remaining alternative solutions are reviewed and analyzed in concert with Specialty Engineering, risk management, lifecycle engineering, and integrated program planning to determine adequacy and suitability of each remaining alternative. The alternatives are pared down to preferred design solutions.

#### **4.5.3.4 Allocate to System Elements—Step 4**

The previous Synthesis steps have resulted in a promising set of conceptual designs for systems satisfying the program requirements for the functional area under consideration. Each design concept must now be developed in more detail so that requirements and design constraints are assigned to the top-level elements of that system design.

##### **4.5.3.4.1 Allocate Requirements to System Elements**

In prior steps, the functional area and associated requirements were adjusted in concert with Functional Analysis and Requirements Management, respectively. As this Synthesis step is entered, the program requirements to be satisfied by the design solution(s) are established, and this step furthers the design process by allocating the requirements to system elements.

These elements are the highest level distinct elements of the system in the areas of hardware, software, and humans in the system. Each system element must perform at least one function within the functional area to be considered separately and distinctly in the traceability of requirements.

The design engineers allocate program requirements to the selected system elements. They document all program requirements that the system must satisfy and formally begin tracking the requirements through the various design and acquisition phases of the system. Documentation includes information regarding the hardware, software, or other system components to which each requirement is allocated.

#### 4.5.3.4.2 Allocate Design Constraints to System Elements

Design constraints that apply directly to system elements are identified. These constraints do not apply to the functions performed, but rather to the elements: hardware, software, or people. Design constraints differ from constraint requirements in that they recognize existing limitations to design of a system, its interfacing systems, and its operational and physical environment. Such design constraints will include power, weight, data throughput rates, memory, and other resources. These constraints represent the system's inability to achieve a capability or level of performance due to such issues as insufficient technology and lack of available facility space for the system.

Design constraints are especially important in analyzing the design of potential replacements for existing systems. This is of particular interest to design engineers when major elements of the original system may be retained. Once allocated, the design constraints will clearly define which system elements remain, are added, or modified.

The technology constraints identified during the prior technology assessment are allocated to the system elements. Those constraints identified during review of Specialty Engineering attributes are also allocated to ensure that inappropriate design characteristics are not introduced into the selected system. Finally, environmental constraints are allocated down to the system element level. Environmental constraints can be introduced by climatic conditions under which the total system will operate, by the facilities in which the system will be housed, or more globally by environmental hazards and constraints (such as Environmental Protection Agency regulations) imposed in the region(s) where the systems will be used.

#### 4.5.3.5 Define Design and Performance Characteristics—Step 5

With the system concepts now defined, identify and document the design and performance characteristics of each alternative. Characterization of the system(s) is all-inclusive and addresses all facets of the system under design, including the associated human-engineering elements and lifecycle considerations or needs.

During this phase, there is substantial benefit to practice concurrent engineering. The entire functionality of the system(s) under design is considered. When the design and performance characteristics are defined, the entire lifecycle of the potential system must be considered—from inception to disposal—in an integrated process. This requires involvement of all Specialty Engineering disciplines (Section 4.8) in the Synthesis process. Thus, sound engineering decisions are made based on strong consideration of all phases and aspects of the system under design consideration.

##### 4.5.3.5.1 Assess Failure Modes and Effects

Failure modes and the effects of failure are assessed for the design alternative. The hardware, software, and human elements of the design alternative are analyzed, and historical or test data is applied to estimate the probability of successful performance of each alternative. Use a failure modes and effects analysis (FMEA) to identify the strengths and weaknesses of the design solution. (See Reliability, Maintainability, and Availability Engineering (subsection 4.8.2) of Specialty Engineering, Section 4.8.) For critical failures, a criticality analysis is conducted to prioritize each alternative by its criticality rating. The analysis results are used to direct further design efforts to characterize redundancy and graceful system degradation elements of the system.

##### 4.5.3.5.2 Assess Testability Needs

The design team analyzes the testability of the design in relation to the operational or maintenance needs. The team determines the need for a built-in test, Remote Maintenance Monitoring, and/or a fault-isolation test for each potential design alternative. Test mechanisms

are considered in the design and incorporated as necessary for elements that are normally maintained by the users or field support engineers. Diagnostic operations to support lower level maintenance actions are likewise incorporated into the design solution.

#### 4.5.3.5.3 Assess Standardization Opportunities

The alternative is assessed for possible use of standardized end items that are technologically and economically feasible. Use of design elements that implement commercial and international standards is strongly considered.

#### 4.5.3.5.4 Assess Lifecycle Factors

The design of each alternative is assessed to determine the degree to which quality factors (producibility, ease of distribution, usability, supportability, trainability, and disposability) have been included in the solution. Additionally, associated lifecycle process needs, requirements, and constraints are identified and defined for each design under consideration. (See Lifecycle Engineering (Section 4.13).)

#### 4.5.3.6 Define Physical Architecture—Step 6

A physical architecture defines and describes the way in which the various functional architecture elements can be assembled to form physical entities. The physical entities must represent a viable design alternative and must provide one or more services that address user needs as translated by the program requirements. The physical architecture may involve such physical entities as runways and various forms of equipment; such nonphysical entities as software; or a combination of the two.

The physical architecture identifies the physical subsystems, and architecture flows between subsystems that will implement the functions and provide the needed services/capabilities. The physical architecture further identifies the system inputs and outputs.

In constructing a physical architecture, use the following definitions.

- **Physical Entities.** The classes of physical entities that will be used are:
  - *Subsystems.* Subsystems are the primary structural components of the physical architecture. They perform functions that “belong” together and whose interfaces require interoperability and compatibility. It is 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.
  - *Users.* These are people who interact with the architecture implementation. They could be either those who use the system (such as the flying public or pilots in the NAS) or operators who use features of the system (such as air traffic controllers in the NAS). Each interface to a user involves human interaction with the system.
  - *External Systems.* These are organizations and agencies (such as Department of Defense or National Weather Service external to the NAS) and/or their systems that will likely interact/interface with the system under design.
  - *Environment.* This is the physical world (e.g., pavement, air, obstacles).
- **Physical Interfaces.** These are mechanical, electrical, data, and other interfaces between system elements or subsystems. Physical interfaces also include all interfaces between the system and its outside world.

#### 4.5.3.6.1 Decompose Into Physical Entities

The architecture can be viewed at several levels of detail. The architecture defines collections of subsystems while defining their interfaces. Consideration is given to a variety of engineering and programmatic disciplines along with stakeholder contributions, and all are incorporated into the physical architecture.

#### 4.5.3.6.2 Define Physical Interfaces

Identify and define the physical interfaces among products, subsystems, humans, lifecycle processes, and external interfaces to higher level systems or interacting systems. Physical interfaces that impact design include communication, data, support, test, control, display, connectivity, or resource replenishment characteristics of the interaction among subsystems, the products, humans, or other interfacing systems or a higher level system. (See Interface Management (Section 4.7).)

#### 4.5.3.7 Analyze and Refine Design Alternatives—Step 7

As a particular design alternative is refined, it is analyzed to determine how it satisfies the allocated functional and performance requirements, interface requirements, and design constraints and how it adds to the overall effectiveness of the system or a higher level system. During analysis, specialty engineers work with design engineers to ensure that requirements such as reliability, availability, maintainability, supportability, safety, human factors, security, electromagnetic compatibility, and spectrum management are incorporated into the design. Additionally, lifecycle process requirements are identified and defined for each alternative system product solution and aggregate of solutions.

##### 4.5.3.7.1 Assess Design Capacity To Evolve

The design alternative is analyzed regarding its capacity to evolve or be reengineered, accommodate new technologies, enhance performance, increase functionality, or incorporate other cost-effective or competitive improvements once the system is in production or in the field. Limitations that may preclude the system's ability to evolve should be identified and the approach analyzed and refined to resolve any limitations. The supportability of an evolving system may require the support process to evolve along with the product. This consideration may significantly affect support funding and training requirements.

##### 4.5.3.7.2 Develop Models and Prototypes

Models and/or prototypes are developed to assist in:

- Identifying and reducing risks associated with integrating available and emerging technologies
- Verifying that the design solution (consisting of hardware, software, material, humans, facilities, techniques, data, and/or service) meets allocated functional and performance requirements, interface requirements, workload limitations, and constraints
- Verifying that the design solution satisfies functional architecture and program requirements

The models, data files, and supporting documentation are maintained, and each version of a model or data file that impacts requirements, designs, or decisions is saved in the integrated database. Models may be digital, partial, or complete and may be hardware, software, or a combination of both; or they may include human models or human-in-the-loop simulations or mockups for usability testing and workload measurement. (See Trade Studies (Section 4.6).)

#### 4.5.3.8 Assess Requirements Compliance—Step 8

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. This is not to be confused with Verification (Section 4.12).

##### 4.5.3.8.1 Perform Design Loop

The design loop involves revisiting the functional architecture to verify that the physical architecture developed is consistent with the functional and performance requirements. It is a mapping between the functional and physical architectures. During Synthesis, reevaluation of the Functional Analysis may be caused by discovery of design issues that require reexamination of the initial decomposition, performance allocation, or even the higher level requirements. These issues might include identification of a promising physical solution or open-system opportunities that have different functional characteristics than those foreseen by the initial functional architecture requirements.

##### 4.5.3.8.2 Perform Requirements Feedback Loop

The system design is audited to determine compliance with the program requirements set. Audits are performed at various levels, from the top-level physical architecture down through each hierarchy level to the lowest-level system element or configuration item. Compliance with program requirements is assessed through both informal and formal reviews. The audit results are then fed back to earlier Synthesis steps as needed, resulting in another Synthesis loop. The audit results may call for program requirement changes at varying levels, or they may lead to design changes to ensure compliance.

#### 4.5.3.9 Select “Best Value” Alternative—Step 9

The “best value” alternative must be the one that offers the most balanced design. The “best value” alternative is selected using all prior analysis conducted in Synthesis or in conjunction with Requirements Management (Section 4.3), Functional Analysis (Section 4.4), Trade Studies (Section 4.6), Specialty Engineering (Section 4.8), and Risk Management (Section 4.10). Upon being selected, the design is detailed and finalized. The designation and description of interfaces (internal and external) among design elements are finalized. The design is baselined and placed under formal configuration management processes.

#### 4.5.4 Process Outputs

It bears repeating that Synthesis is an iterative process, concurrent with Functional Analysis (Section 4.4) and Requirements Management (Section 4.3). The engineering team must use good judgment in aligning the degree of detail of the Synthesis outputs with the position of the project in the AMS cycle.

Prior to selection of the “best value” alternative, Synthesis outputs are completed concisely and at a very high level for *all* possible solutions. As the functional analysis and program requirements become more specific, there will be fewer and fewer alternative solutions that answer the need. As the process narrows toward the “best value” alternative, the top choices will have detailed, documented outputs from the Synthesis team. Once the Joint Resources Council chooses the preferred solution, the Synthesis team will complete the definition of the design process down to the very finest detail.

Therefore, the following Synthesis outputs occur throughout the iterative process, but they vary in scope and detail based on the project’s position within the AMS cycle.

#### **4.5.4.1 Physical Architecture**

For all the alternative solutions, the system elements are identified along with their arrangement and the interactions between them. A description of the salient features of the overall solution is developed as well as descriptions for the system elements and their relationships establishing a potential system architecture baseline. The descriptions are diagrams, schematics, concept drawings, tabular data, and narrative reports.

The design architecture is established at a level that documents the design solution and interfaces. It includes the requirements traceability and allocation matrices, which capture allocation of functional and performance requirements among the system elements. Design architecture definitions should be stored in the integrated database along with tradeoff analysis results, design rationale, and key decisions to provide traceability of requirements up and down the architecture. Verification of the design architecture should be done to demonstrate that the architecture satisfies both the validated program requirements and the verified functional architecture. This information is further compiled into a Requirements Compliance Matrix.

#### **4.5.4.2 Description of Alternatives**

##### **4.5.4.2.1 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.

##### **4.5.4.2.2 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.

##### **4.5.4.2.3 Schematic Block Diagrams (SBD)**

The SBD illustrates the physical partitioning and interfaces for each viable candidate hardware and software design solution. SBDs should not be developed for every conceivable design—only for those that are worthy of detailed evaluation (based on position within AMS cycle).

##### **4.5.4.2.4 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 4.7).

#### **4.5.4.3 Product Definition**

The drawings, schematics, software documentation, manual procedures, and so on are developed as necessary to document the selected design elements in a product definition.

##### **4.5.4.3.1 Configuration Item Descriptions**

Each of the system elements is identified during the Synthesis process. This includes all hardware configuration items (HWCI) and computer software configuration items (CSCI). Each HWCI and CSCI is documented and described at the time of its summary or preliminary identification. Once the “best value” alternative is selected, detailed documentation for each

HWCI and CSCI of the selected system is developed, thus establishing a configuration baseline for the system. (See Configuration Management (Section 4.11).)

#### **4.5.4.3.2 Specification Inputs**

During Synthesis, compliance with the program requirements (Requirements Verification Compliance Document (RVCD)) was assessed. This analysis sometimes results in recommendations for modification or elimination of requirements. Any proposed modifications or deletions are documented and forwarded to Requirements Management (Section 4.3).

#### **4.5.4.3.3 Requirements Compliance Matrix**

All requirements have been mapped to the system elements. As the mapping occurred during Synthesis, a matrix was developed containing all requirements, the subsystem or element 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. Compliance levels are determined using system/cost-effectiveness analysis, simulations, demonstrations, inspection, and/or testing.

#### **4.5.4.3.4 Refined Work Breakdown Structure (WBS)**

The selected design's physical architecture is used to refine the WBS by translating the decomposition into a WBS format. The refined WBS provides enhanced work planning, cost/schedule tracking, and control by extending the existing WBS to account for the system elements identified during Synthesis.

#### **4.5.4.4 Constraints**

Constraints are formed before the program enters the Synthesis process, and yet more may be identified during the process. Synthesis looks at many different aspects of the system design, including cost, scheduling, feasibility, requirements, function, and others. As various solutions to the Mission Need Statement are considered and refined, constraints become apparent.

Constraints are clearly seen when performing step 4, "Allocate to System Elements" (subsection 4.5.3.4), of the Synthesis process. The constraints identified may cause iteration through the design feedback loop or the requirements feedback loop. An evolutionary development is initiated, if necessary, for any design element for which a lesser technology solution was selected over a higher risk technology, and for which the capacity to evolve was designed into the element and interfacing elements. (See Trade Studies (Section 4.6)).

##### **4.5.4.4.1 Design Constraints**

Step 5, Define Physical Architecture (subsection 4.5.3.5) identifies and documents constraints specific to the Synthesis process. These design constraints do not apply to the functionality of the system, rather they are in the area of hardware, software, or people. Because these design constraints are so important in analyzing replacement of existing systems, they are documented and sent on for further study in the Lifecycle Engineering process (Section 4.13), aiding in identifying the timing of future replacement schedules. Additionally, these design constraints become another output of the Synthesis process, as requests for a Trade Study (Section 4.6) evaluation are sent out.

##### **4.5.4.5 Planning Criteria**

Planning criteria describing planned activities for the Synthesis process are output to the Integrated Technical Planning process (Section 4.2).

#### 4.5.4.6 Tools/Analysis Requirements

Tools/Analysis Requirements for performing Synthesis throughout the remainder of the program's lifecycle need to be provided to the Integrity of Analysis process (Section 4.9).

#### 4.5.4.7 Concerns and Issues

Appendix D contains guidance on Concerns and Issues as a product of Synthesis and how to best convey that information to the Risk Management team (Section 4.10).

#### 4.5.5 Metrics

Performance of the Synthesis process itself shall be measured on a regular basis and recorded in the metrics library monthly. The following metrics, at a minimum, will be used to evaluate performance:

1. Trade Study Satisfaction Assessment (see Trade Studies (Section 4.6))
2. For approved engineering problem reports:
  - a. Quantity, by type of problem report
  - b. Cycle time from disposition to incorporation of change into released engineering documents, by type of report
3. Technical Performance Measurements: objective versus achieved values
4. Number of approved engineering changes: by product, type, and stage
5. Documents/drawings submitted for engineering release:
  - a. Unacceptable submittals
  - b. Total submittals
6. Number of technical action items identified during reviews and audits
7. Design efficiency metrics, such as weight, required power, and envelope dimensions (volume)
8. Cost and schedule variance for completion of Synthesis steps
9. System requirements not met
10. Number or percent of system requirements verified by system analyses
11. Number of items yet to be determined within the system architecture or design
12. Number of interface issues not resolved
13. Percent of identified system elements that have been defined

#### 4.5.6 Tools

##### 4.5.6.1 Schematic Block Diagrams

Along with the definition of design alternatives, it is important to establish the relationships between alternatives at each level of design activity. One can use SBDs to accomplish this.

A simplified 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 (see Functional Analysis (Section 4.4) for examples) 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, as part of subsection 4.5.3.6 (Define Physical Architecture) of the Synthesis process, 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.

#### 4.5.6.2 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.

#### 4.5.7 References

1. Blanchard, Benjamin S. *Systems Engineering Management*. Second Edition. New York, NY: John Wiley & Sons, Inc., 1998.
2. Defense Systems Management College. *Systems Engineering Fundamentals*. Fort Belvoir, VA: Defense Systems Management College Press, 1999.
3. *European ITS Framework Architecture, The KAREN Project—Physical Architecture*, Version 2. European Communities, Keystone Architecture Required for European Networks (KAREN), August 2000. ([http://www.frame-online.net/Karen\\_doc/d36a1fin.pdf](http://www.frame-online.net/Karen_doc/d36a1fin.pdf))
4. *Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications*. DO-264. Prepared by SC-189. Washington, DC: Radio Technical Commission for Aeronautics, Inc. (RTCA), December 14, 2000.
5. *IEEE Std-1220-1998, IEEE Standard for Application and Management of the Systems Engineering Process*. Los Alamitos, CA: Institute of Electrical and Electronics Engineers, 1998.
6. *International Council on Systems Engineering (INCOSE) Systems Engineering Handbook*. Version 2.0. Seattle, WA: INCOSE Central Office, 2000.
7. Martin, James N. *Systems Engineering Guidebook: A Process for Developing Systems and Products*. Boca Raton, FL: CRC Press LLC, 1997.
8. *National ITS Architecture Documentation, Physical Architecture*. Lockheed Martin Federal Systems, Odetics Intelligent Transportation Systems Division. Washington, DC: ITS America, September 1998.
9. *Processes for Engineering a System*. EIA-632. EIA Standard. Arlington, VA: Electronic Industries Alliance, January 7, 1999.
10. Sage, Andrew P., and Rouse, William B. *Handbook of Systems Engineering and Management*. New York, NY: John Wiley & Sons, Inc., 1999.

11. *Systems Engineering Capability Model*. EIA/IS-731.1. EIA Interim Standard. Arlington, VA: Electronic Industries Alliance, December 1998.
12. *Systems Engineering Guidebook for ITS*. Version 1.1. California Department of Transportation, Division of Research and Innovation, February 2005, page 197.

## **4.6 Trade Studies**

Trade Studies is the System Engineering (SE) element that multidisciplinary teams use to identify the most balanced technical solutions among a set of proposed viable solutions. It is a key tool in developing designs that meet stakeholder requirements in the most cost-efficient manner possible. The application of Trade Studies prevents program/project management from committing too early to a design that may not be cost effective or meets all system requirements. Through Trade Studies, desirable and practical alternatives that better combine cost and effectiveness may be identified, resulting in beneficial selections among the alternatives. Figure 4.6-1 depicts the Trade Studies Process-Based Management chart.



**Process:**  
 Perform Trade Studies

**ID No.:** 4.6 (iCMM PA 4)  
**Date:** April 19, 2000  
**Revision Date:** August 30, 2006

**Next Higher Level Process:**  
 Perform System Engineering

**Process Owner:**  
 System Engineering Council

**Process Objective:**

Select most balanced (cost, schedule, quality, and risk) solutions from a set of proposed viable alternatives based on defined criteria.

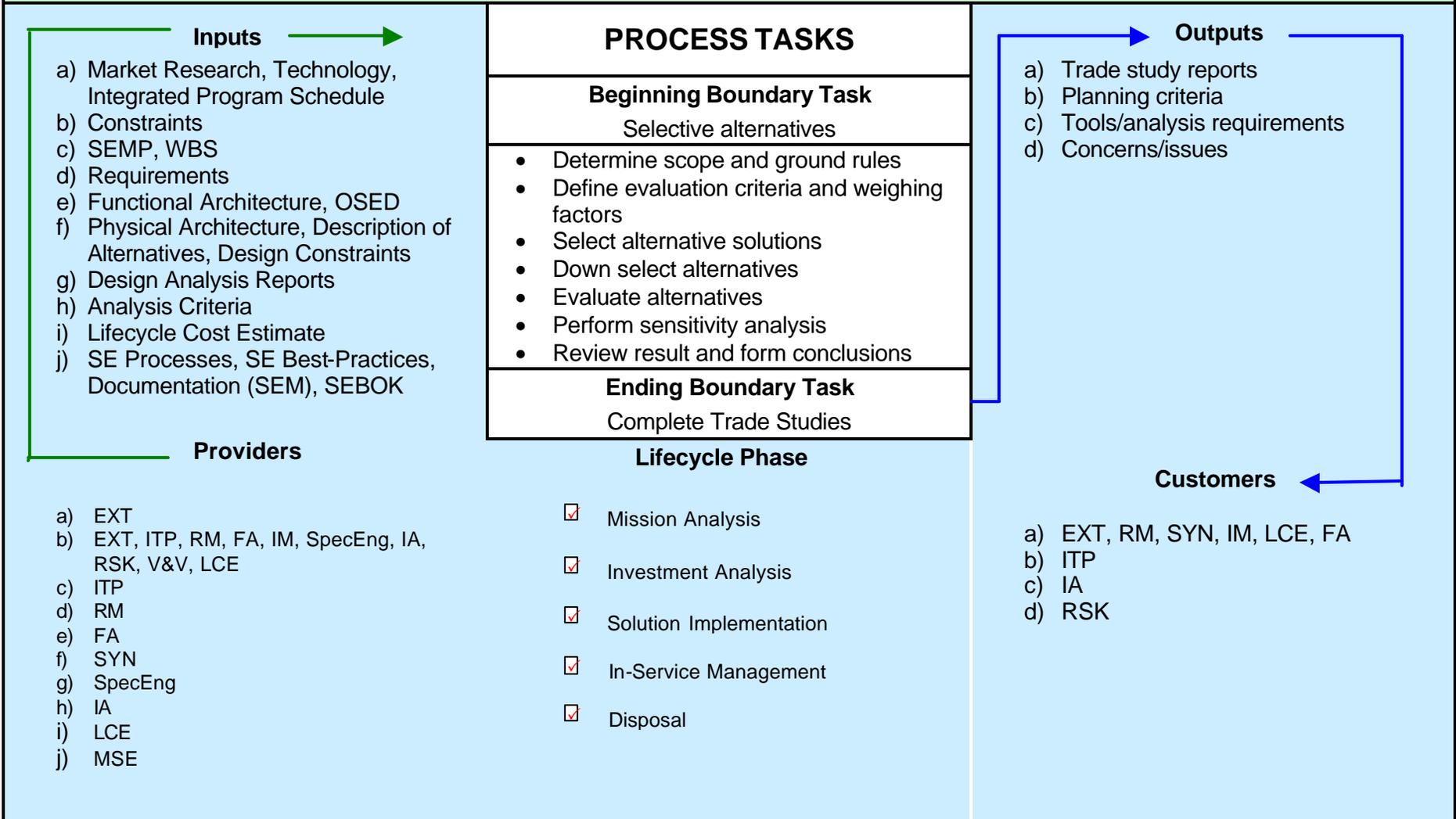


Figure 4.6-1 Trade Studies Process-Based Management Chart

Conducting Trade Studies involves evaluating two or more alternatives to select a preferred option. The Trade Studies process balances such considerations as cost, reliability, testability, supportability, survivability, compatibility, and producibility during each phase of the product development cycle.

A disciplined Trade Studies process is required to fairly evaluate alternative concepts and designs. The process requires that any affected discipline participate in the program/project to the extent needed to arrive at the best-balanced requirements solution. Typically, a Trade Studies leader, who is not a stakeholder in any of the proposed solutions, helps to focus and coordinate the flow of information that occurs during the Trade Studies process.

Trade Studies may be formal and informal, with different emphases, depending on when in the program lifecycle they are conducted. It is appropriate to develop a Trade Studies plan (Integrated Technical Planning (Section 4.2)) for each major problem or issue for which alternatives are being considered.

This section describes the Trade Studies process as a formal decision making methodology used to select among alternative concepts, designs, products, or approaches that satisfy the system implementation and to resolve any conflicts that arise during the system's lifecycle.

#### **4.6.1 Introduction to Trade Studies**

Trade Studies are conducted within and across disciplines to support decisions at any phase of the program's lifecycle. The process quantifies and/or qualifies the consequences of selecting various system alternatives in terms of metrics that are traceable to customer requirements and are declared by project management to be project objectives. They support the allocation of performance requirements and the determination of design constraints and are used in evaluating alternative functional architectures obtained from Functional Analysis (Section 4.4). In general, the results of the Trade Studies process may be quantitative or qualitative in nature.

Trade Studies may be performed at any step in the system's lifecycle, but the process begins at the Mission Analysis phase and continues through first article production. For example, the major goal of the Investment Analysis (IA) phase is to define a set of system requirements that meets the goals and objectives of a mission or a system at an affordable cost and with an acceptable level of risk. During this phase, Trade Studies may be used to select among competing sets of requirements that define alternative system concepts. In a similar manner, the Trade Studies process is used to assist SE.

The following list summarizes the use and emphasis of Trade Studies in the program's lifecycle:

Mission Analysis phase:

- Define mission requirements
- Resolve conflicting high-level customer requirements
- Evaluate alternative high-level requirements to meet mission needs

IA phase:

- Compare technologies and approaches

- Evaluate concepts to meet high-level requirements
- Select alternative system configurations for further study
- Select concept for preliminary design development and conceptual layouts
- Support Functional Analysis (Section 4.4) and allocation of performance requirements (alternative architectures)
- Establish system configuration
- Support decision for new product development versus nondevelopment products
- Establish system, subsystem, and component configurations
- Select testing methods
- Determine installation locations; check for fit and compatible environment
- Detail design
- Define a best-value design solution that satisfies all system requirements
- Support detailed design analysis
- Compare manufacturing processes
- Determine best order of assembly

Solution Implementation phase:

- First article, full-scale development
- Resolve unexpected manufacturing issues, such as changing the order of assembly or revising a manufacturing process
- Select alternative designs, solutions (operations, maintenance, integrated logistic), procedures, and configurations

#### 4.6.1.1 Trade Studies Objectives

Trade Studies are conducted at the program's different lifecycle stages to discover the best-value solution, best value to the government, and best value to a set of requirements from technical, cost, or schedules points of view. Trade Studies, also referred to as tradeoff studies or selection studies, are performed for a variety of purposes, including to:

- Choose among alternative design and implementation strategies and solutions based on architecture, performance, and cost in order to meet stakeholder requirements
- Recommend commercial-off-the-shelf (COTS) products for acquisition
- Perform make-versus-buy analyses, or buy-versus-lease analyses (Office of Management and Budget Circular A-76, Outsourcing Decision)
- Recommend a supplier for services
- Document and justify the selection of a solution for a system requirement
- Reduce risk

Trade Studies provide an objective determination of comparative metrics for various system options. An essential aspect of the analyses performed for these studies is that consistent,

configuration-controlled parameters be used in the computations to ensure comparison of likely system solutions.

#### **4.6.1.2 Participants**

All elements of the project organization are responsible for Trade Studies. The process requires the participation of various interdisciplinary skills in an integrated manner with the objective of producing an optimum system design.

Design, manufacturing, test, operations, and product support perform lower level Trade Studies that involve subsystems, components, subcomponents, and software. In the event of utilization of system-level resources contention, program/project management coordinates with the stakeholder organizations to resolve issues and establish priorities. It is recommended that Trade Studies affecting hardware and software account for system issues related to software, operations, procedures, training, and other non-material-related solutions.

To determine impacts across interfaces, it is recommended that SE integrate the Trade Studies performed by various groups.

#### **4.6.2 Inputs to Trade Studies**

Inputs to the Trade Studies process may be divided into two categories: stakeholders and project. The stakeholder inputs include the operations concept, program requirements, and system requirements. The project inputs include design analysis report (DAR), Functional Architecture (Section 4.4), DAR (Section 4.8), results from Validation and Verification (Section 4.12), and Lifecycle Cost Estimates from Lifecycle Engineering (Section 4.13).

The Trade Studies process presupposes that alternatives have been identified that are evaluated as specified by the process objective. To complete this task:

- Requirements, Constraints, expectations, assumptions, goals, and regulations shall be clearly understood
- Design options, including baseline and other criteria, shall be provided or developed
- Relevant plans and documents shall be provided

#### **4.6.3 Trade Studies Process Tasks**

The methodology to evaluate system alternatives is described in the following subsections. The Trade Studies process consists of the following tasks:

- Determine scope and ground rules
- Define evaluation criteria and weighting factors
- Select alternative solutions (brainstorm possible solutions), if not provided
- Down-select alternatives
- Evaluate alternatives
- Perform sensitivity analysis
- Review results and form conclusions

- Document the Trade Studies

These steps seldom are performed sequentially. Certain steps, such as definition of evaluation criteria, may be repeated several times as alternatives are defined and evaluated. Figure 4.6-2 depicts the overall Trade Studies process.

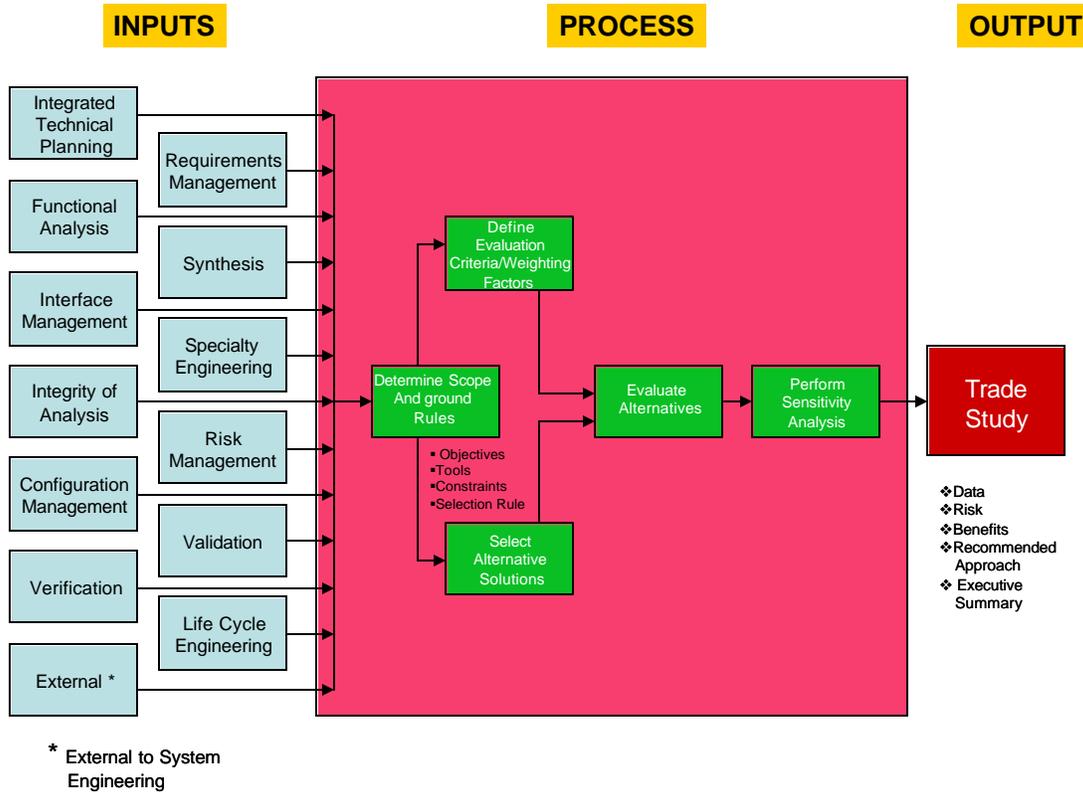


Figure 4.6-2. Trade Study Process

#### 4.6.3.1 Task 1: Determine Scope and Ground Rules

To complete Task 1, perform/consider the following checklist of actions/issues:

- Determine the specific goals of the Trade Studies and the Requirements to be met before establishing the scope and methods of the study:
  - Consider all viewpoints of stakeholders (e.g., users, developers, managers, and operations and maintenance personnel) to accomplish this goal
  - Ensure that input is obtained from all customers associated with the study and that the stakeholders' viewpoints are clearly understood and documented
  - Understand and resolve differences between competing viewpoints and any underlying biases before continuing the evaluation process
- Use the methodology described in Requirements Management (Section 4.3) to define and analyze the Requirements for the Trade Studies:
  - Select Requirements to bound the Trade Studies into four major categories: functional, performance, operational, and programmatic

- Base the Requirements on the goals established for the study and adjust the level of detail of the Requirements to the scope of the particular study
- Ensure that the Requirements, which are used as a basis for criteria against which alternatives are evaluated, are accurate, unambiguous, verifiable, complete, and appropriate
- Obtain the customer's approval on the goals and Requirements for the tradeoff study
- Define the system's goals and objectives and identify the Constraints to satisfy:
  - Recall that in the early phases of the system's lifecycle, the goals, objectives, and constraints are usually stated in the operational terms; when the system architecture and design have been determined or established, the goals and objectives are usually stated as performance requirements.
- Spend time upfront clearly defining the problem and jointly coordinating with the respective internal and external customers regarding the key Requirements that any solution needs to meet. Achieving consensus with affected team leaders regarding the real problem to be resolved saves significant time in the overall process.
- Establish a multidisciplinary team that is able to support the analysis effort from start to finish. Having expertise within each discipline ensures that alternatives are thoroughly evaluated, leading to the most accurate assessment results. Available budget and time control most studies; therefore, when equipped with this information, team members realize how far they may pursue alternatives.
- Develop an attainable schedule as well as identify major Trade Studies milestones. It is recommended that the degree to which excursions from the baseline concept are allowed also be defined. A study lacking clear boundaries easily grows far beyond the available resources.

It is recommended that the Trade Studies team leader coordinate items that influence subsystems and assess the impact on his/her area. It is also recommended that subcontractors, as well as those on the Trade Studies team, consider and identify previously developed hardware and software components, non-developmental items, and COTS hardware and software as candidates for utilization in the Trade Studies. Additional items for the team to consider and identify are common components in different parts of development to share across development groups or across configuration items.

Before the Trade Studies process is conducted, the decision-making body responsible for the affected baseline shall approve the Trade Studies plan.

#### **4.6.3.2 Task 2: Define Evaluation Criteria and Weighting Factors**

The definitions of measures and measurement methods for system effectiveness, system performance, and system cost are related to the definition of goals and objectives and Functional Analysis (Section 4.4) performance. These measurements are the decision criteria. Each quantitative measure shall have a defined measurement or computational method. This task initiates the analytical portion of the Trade Studies process, as it involves using quantitative methods.

The definition of evaluation criteria requires considerable engineering judgment and interaction with the stakeholder to establish the appropriate criteria, associated weights, and scoring

methods. For example, supporting missions with tight schedules requires heavy weighting of schedule risk, while supporting missions with more flexible schedules generally emphasizes low cost while accepting higher schedule risks. Sufficient comments shall be provided for each evaluation criterion to ensure evaluator and stakeholder comprehension. Stakeholder approval shall be obtained before proceeding to the next task.

The technical requirements that potential solutions need to achieve serve as the criteria against which alternative concepts are measured. The selected criteria may include limits of minimum acceptable values and desirable attributes that permit judging of candidates against each other. Trade Studies leaders are encouraged to use Quality Function Deployment (QFD) to help to define the evaluation criteria and weighting factors applicable to the Trade Studies. These criteria are defined based on the technical requirements that determine if a design is acceptable to the Stakeholder Needs.

Evaluation criteria are more meaningful if they represent measurable characteristics, which is not always possible. It is recommended that criteria on cost and risk be included. Alternatives may be evaluated based on projected fixed and variable cost using risk factors, when applicable, to derive expected costs. It is also recommended that elements not directly related to cost (e.g., weight, production cycle time) have criteria established to associate cost with changes in the elements. Trade Studies shall address these criteria.

An experienced, multidisciplinary team shall brainstorm a list of additional criteria suitable for the study's intent if all feasible alternatives are to be identified and thoroughly evaluated. Each criterion shall be described to a level of detail such that its intent is clear to all team members. This detail ensures that all participants are well aware of specified and derived Requirements affecting evaluation.

When a particular study is planned, the effort and cost of that study shall be balanced against the impact (e.g., cost, schedule, and technical risks) on the study's scope and methodology. An overly ambitious and costly study among low-impact alternatives is as serious as the failure to adequately evaluate high-impact alternatives. For a simple evaluation of several low-impact alternatives, subjective evaluation and consensus may be sufficient. For complex studies with higher impact, the following is recommended:

- Define evaluation criteria based on the Requirements analysis
- Determine relative weights for the evaluation criteria based on the Requirements analysis
- Prepare a scoring matrix that assigns a row for each evaluation criterion and a column for each alternative to be evaluated, with comment fields for each criterion
- Define a method for assigning a score to each element in the scoring matrix
- Assign a score for each criterion for each alternative:
  - Select scores in such a manner that the higher the score, the more favorable the evaluation; use an odd number of integers so that the middle score represents an average rating
  - Use small integers, typically 0 to 5, to represent scores; a range of 0 to 2 may be adequate; a range in excess of 0 to 10 is not recommended
  - Determine a method of recording items that is unable to be scored; define the scoring method to be used; recording a blank for unknown information often is useful

- Prepare a weighted score matrix that assigns a row for each evaluation criterion and its weight and assigns a column for each alternative to be evaluated. The weighted score recorded for each element in the matrix is the product of the weight for that criterion and the corresponding score in the scoring matrix.

Figure 4.6-3 is a sample decision analysis matrix.

Decision Factors \ Alternatives	Decision Factor 1		Decision Factor 2		...	Decision Factor n		Total Weighted Score
	Weight = 1		Weight = 1.5		...	Weight = 2.5		
	Score	Weighted Score	Score	Weighted Score	...	Score	Weighted Score	
Alternative 1	7	21	4	6	...	8	20	47
Alternative 2	8	24	10	15	...	10	25	64
⋮	⋮	⋮	⋮	⋮	...	⋮	⋮	⋮
Alternative n	10	30	5	7.5	...	12	30	67.5
Alternative n+1	⋮	⋮	⋮	⋮	...	⋮	⋮	⋮

Figure 4.6-3. Decision Analysis Matrix

Stakeholder approval of the proposed evaluation method shall be obtained.

Stakeholders and internal technical experts are used to establish meaningful evaluation criteria. Criteria for which all potential alternatives are equal in value are not used in the evaluation because they do not add value to the process.

Defining evaluation criteria often requires several iterations before the final criteria are determined. Evaluation criteria are defined based on the analysis of Requirements. Bias shall be avoided when evaluation criteria are established (e.g., acceptance of an existing system or product as the de facto standard for evaluation). The following evaluation criteria are applicable to a wide range of Trade Studies:

- Development cost
- Lifecycle cost
- Requirements compliance
  - Functional
  - Performance
  - Operational
  - Programmatic
- Technical risk (Maturity)
  1. Reliability, Maintainability, Availability

2. System Safety
  3. Quality
  4. Human Factors
  5. Electromagnetic Environmental Effects
  6. Hazardous Materials
- Budget risk
  - Schedule risk
  - Operational complexity
  - Vendor assessment
  - System maturity
  - Development support tools
  - Test support tools
  - Development team familiarity with candidate hardware and software
  - Quality of logistics support

Evaluation criteria that apply specifically to the Trade Studies shall be selected, adding additional relevant criteria, such as security, as needed. For each evaluation criterion, established threshold values that may be used to evaluate the alternatives on a pass/fail basis shall be identified. An example criterion is: "The system MTBF shall be 10,000 hours or greater." For the remaining criteria, a weight and scoring range shall be assigned for use with the weighted matrix evaluation method.

Criteria are ranked and grouped into three categories so that the assigned weights reflect their criticality. The most critical criteria are assigned large weights and flagged so that any alternative with low scores for these criteria influence any subsequent analysis. Mid-critical and noncritical criteria are assigned smaller weights; it is recommended that noncritical criteria have a negligible effect in further analysis.

#### **4.6.3.3 Task 3: Select Alternative Solutions**

Once the evaluation method is established, all available resources are used to develop viable alternatives and solutions. Trade publications, prospective bidders for service contracts, 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., architectures, designs, COTS products).

Based on defined ground rules, the alternative development phase is intended to evaluate multiple alternatives and narrow the prospects for extensive evaluation. The importance of creativity is especially emphasized, as this task may or may not affect the alternative design solutions previously submitted.

The evaluation criteria and detailed Requirements shall be used to synthesize alternative solutions. In defining alternative approaches, developing the alternatives often requires lower level Trade Studies, which enables a hierarchy of design alternatives. A trade tree that

reflects the complete hierarchy of trades to address when performing the top-level Trade Studies shall be drawn. The trade tree shall contain a number of high-level system architectures, which prevents focusing on a single architecture. To eliminate undesirable alternatives, for each trade item in the trade tree, the tasks in the subsections above shall be repeated until a complete trade tree is generated, and the objectives, Requirements, evaluation method, and evaluation criteria are defined. Top-level objectives and Requirements are allocated to successively lower levels of Trade Studies in the trade tree. The allocated objectives and Requirements are used to define the evaluation methodology and criteria, and evaluation is performed, as described in the following paragraphs.

Each design alternative shall be thoroughly assessed. Potential design approaches for each Requirement shall be reviewed against potential approaches for other Requirements in order to identify possible interactions. It is recommended that interactions that might affect the cost of a solution or make one feasible, be documented and handled as linked decisions throughout the Trade Studies process.

Often, risk is the deciding factor in candidate selection. A complete technical analysis identifies and quantifies technical risks and develops contingency alternatives. Therefore, the technical and schedule risks associated with each candidate system are identified, and the probable gain and loss for each risk are analyzed. Also, an acceptable level of risk for a given gain is defined, and efforts are undertaken to minimize new, unproven, complex, or unusual Requirements for hardware, software, and firmware. The use of untried elements is minimized by recommending proven substitutes whenever possible.

A technical analysis of schedule risk areas is performed, and all long-leadtime items, which are the schedule drivers, are identified. How the design affects the development schedule is discovered, and all system elements and resources that may be available when needed are determined. All single-source items that may be potential risks are identified, and a recommended level of schedule contingency, as appropriate, is defined.

Expected operational scenarios for each candidate system to assess the interactions of the design alternatives are defined. Also, the expected system growth over the planned system life is determined to assess system design flexibility and expandability. Because system sizing is based on the anticipated workload, every effort to ensure an accurate workload forecast is made, as improperly sized systems result in unnecessary cost and/or insufficient capacity. Human workload and scenario definitions are used as drivers to assess performance, utilization, and capacity of the system under anticipated operational conditions. (Specialty Engineering (Section 4.8) provides guidance on this topic.)

Once a set of possible alternatives has been selected, the next task is to collect data on each to support the evaluation of the measures by the selected method. The data collection, directed by the Trade Studies leader, emphasizes the role of the disciplines, such as reliability, maintainability, integrated logistics, producibility, software, testing, operations, and costing. Figure 4.6-4 is an example of a Trade Studies table.

Criteria	Alternative 1	Alternative 2	---	Alternative N
Cost ▪Initial ▪Recurring	High low	Medium Low	---	Low Low
Performance	Low	High	---	New Design
Reliability Maintainability Availability	Medium	High	---	Medium
Risk ▪Cost ▪Technical	Low (20%) Low (25%)	Low (10%) Low (20%)	---	Low (10%) Medium (35%)

Figure 4.6-4. Example Trade Study Table

#### 4.6.3.4 Task 4: Down-Select Alternatives

When numerous possible alternatives are identified, a detailed analysis of each one may not be cost effective; therefore, down-selection of candidates is recommended. Identifying high-risk candidates and candidates with questionable feasibility or high lifecycle cost helps to reduce the number of alternatives to be studied. Screening the alternatives against the selection criteria eliminates these candidates. If one of a closely grouped set of alternatives is down-selected, it is recommended that all alternatives in that group be down-selected. Any relationship that is not the same for each down-selected alternative and the baseline becomes part of the detailed Trade Studies. Each alternative is defined to an appropriate level of detail to differentiate the alternative with respect to the technical requirements, which typically include layouts, tooling concepts, cost studies, and other detailed analysis. When only the down-select Requirements are the focus, the effort is simplified to only those Requirements that are different among the design alternatives and the baseline.

The down-selected alternatives are provided to all disciplines involved to ensure that each has the opportunity to evaluate the impacts. This process provides discrete impacts for each area used to select the preferred alternative. It is recommended that this process be performed in parallel with each discipline preparing its inputs simultaneously.

#### 4.6.3.5 Task 5: Evaluate Alternatives

The next task in the Trade Studies process is to quantify the outcome variables by computing estimates of system effectiveness, underlying system performance or technical attributes, and system cost. If the needed data has been collected and the measurement methods (e.g., models) are in place, this step, in theory, is mechanical. In practice, considerable skill often is needed to obtain meaningful results.

Recommended actions include the following:

- Perform a detailed evaluation of all approved viable alternatives. An individual or a small group may perform this evaluation. Record any problems or questions. If a weighted matrix method is used, finish scoring without reference to weights or flags.

- Evaluate the alternative approaches relative to the evaluation criteria when performing the Trade Studies process
- Identify any alternatives with high-weighted scores that narrowly failed the pass/fail criteria. Discuss these alternatives with the stakeholder.
- Evaluate cost factors separately from the remaining evaluation criteria throughout the process. In some cases, none of the alternatives may satisfy all pass/fail criteria. In such cases, relax one or more pass/fail criteria, investigate additional alternatives, or report to the stakeholder that no entirely acceptable alternative has been found.

Ideally, all input values are precisely known, and models perfectly predict outcome variables. Since this case is not typical, it is recommended that the Trade Studies leader supplement point estimates of the outcome variables for each alternative with computed or estimated uncertainty ranges. For each uncertain key input, it is recommended that a range of values be estimated. Using this range of input values, the sensitivity of the outcome variables may be gauged, and their uncertainty ranges calculated.

The baseline reference method, relative rank method, and cost assessment method are several methods used to evaluate alternatives and are discussed in the following subsections.

#### **4.6.3.5.1 Baseline Reference Method**

The baseline reference method requires a baseline or legacy design and a set of associated databases on the use of that design. Alternatives are evaluated against the baseline design or other reference using the selected evaluation criteria. If an alternative is clearly better than the baseline, it is marked as a plus (+); clearly worse than the baseline (-); same as baseline (S); and unacceptable as the baseline (U). This evaluation requires a team effort of all disciplines participating in the study, with team agreement for each rating. It is recommended that notes be maintained as to why ratings are given for each relationship. Using numbers or ++/-- may expand the sensitivity of the +/- system. However, doing so slows the evaluation process and places dangerous emphasis on the matrix as a tool that delivers answers more definitive than the process warrants. When making the +/- decision, the magnitude of the difference shall be considered; however, the process of marking an only marginally better feature as + compared to the baseline shall be avoided.

Generally, alternatives with a U relationship are eliminated, or the U condition is removed; however, there are exceptions to this rule. An exception may be when the Trade Studies process is conducted to determine whether there are sufficient benefits from an alternative to justify a request for a specification change. Also, an alternative in a study may present itself that significantly improves the overall system performance but requires a specification change. It is recommended that common sense be used when U relationships are evaluated and that the users' needs be considered.

Once relationships are defined for each alternative and technical requirement, the overall value of merit of the alternative is calculated. A value of +1 is assigned to each (+) rating, and a -1 to each (-) rating. A relative weight may also be assigned to each evaluation criterion if not all criteria are considered equal. QFD may help to determine this importance weighting.

It is recommended that the following actions be taken when the baseline reference method is used:

- **Multiply the importance weighting and the evaluation and then perform the sum calculation for each alternative.** No calculation is performed for the same evaluations because this method of evaluation is relative to the baseline. The overall importance rating is a figure of merit for each alternative. The higher the importance rating, the better the alternative for the given design requirement. However, this guide is only relative. Do not differentiate alternatives by closely grouped importance ratings. If, for example, three concepts fall in a range of 10-20 and the other is -30, the alternatives in the group 10-20 are basically equivalent.
- **Review each alternative to gain an overall understanding of the meaning of the final importance rating.** It is recommended that the team review all the alternatives with negative relationships and develop supplemental alternatives that eliminate these negatives, resulting in additional viable alternatives. Some of these alternatives use portions of the previously developed alternatives. The development and evaluation of subsequent alternatives shall follow the procedures used for initial alternative development. When supplemental alternatives are developed, low sensitivity of the +/- system is avoided. Developing supplemental alternatives is critical to a successful Trade Studies. A "zero change" option normally is included for comparison.

#### 4.6.3.5.2 Relative Rank Method

The relative rank method uses the Kepner and Tregoe technique to evaluate alternatives. This technique evaluates each alternative against the selected criteria and establishes a ranking for each criterion. Weighting of the criteria is defined by category, while the trade options are graded in their appropriate columns according to the scaling factors over the range 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 for a total.

#### 4.6.3.5.3 Cost Assessment Method

The cost assessment method is similar to the baseline reference method, except that the alternatives are reduced to rough order of magnitude (ROM) estimates of fixed and variable costs. Elements that do not reduce directly to cost (e.g., weight, production cycle time) are translated to cost using common criteria described in "Task 2: Define Evaluation Criteria and Weighting Factors" (subsection 4.6.3.2). If risks are present, risk projections are used to calculate an expected value.

As cost is a major factor in selecting among candidate systems during system design, development, implementation, and operational costs shall be considered when the lifecycle costs of candidate system configurations are evaluated. A refinement of earlier ROM cost estimates is required to complete the information needed to select the system configuration. It is recommended that the estimate include estimates submitted by major subcontractors and vendors and contain sufficient cost detail to answer client questions.

In addition, it is recommended that the following actions be taken when the cost assessment method is used:

- Determine the relative complexity and risk of each candidate system configuration.
- Identify how each candidate system configuration proposes to handle stringent system requirements, such as response time, transaction processing time, and throughput.

- Analyze how each candidate configuration meets special system requirements for a high level of reliability and availability or for quick recovery or automatic failover.
- Highlight key factors that result in lower cost and risk. Discuss the factors with the stakeholder, including the option of analyzing a more simple system that addresses only the most critical requirements set. This type of analysis gives the stakeholder a minimum system cost benchmark to assess cost of the candidate system and functionality of each requirement.
- Include the tradeoffs among hardware, software, and manual operations as part of the cost analysis, and identify the most sensitive cost drivers of each candidate system. If the system has security requirements, also consider security cost drivers.

#### 4.6.3.6 Task 6: Perform Sensitivity Analysis

Sensitivity analysis is used when the solutions are nearly equivalent in scoring and, in some cases, may be required even if the scoring is equivalent.

Recommended actions include the following:

- If using a weighted matrix evaluation method, 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 evaluators. For each compliant 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 weighted scores of varying weights. If some weights are determined by compromise, the range of reasonable values discussed during the definition of evaluation criteria (subsection 4.6.3.2 above) provides useful guidance for such variation.
- 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 evaluated for each criterion. Compute the upper and lower bound for weighted scores (and groups of weighted scores). Document the data in a matrix corresponding to the score and weighted score matrices.
- By inspecting or using a suitable statistical test, determine if any of the variations are large enough to require special attention (i.e., more detailed investigation to ensure the accuracy of the evaluation).
- Evaluate the effect on weighted score totals, including or excluding criteria flagged as noncritical.

Typical outcomes of the sensitivity analysis and review of results include the following:

- **Case 1:** One alternative emerges as the optimal choice if it meets all critical requirements, has the highest weighted score (with a range that does not overlap the range of another alternative), and has the lowest cost.
- **Case 2:** A cluster of alternatives is acceptable (i.e., each alternative in the cluster satisfies all critical requirements, its weighted scores have overlapping ranges, and its cost is competitive).

- **Case 3:** No single, entirely satisfactory alternative is found.

Case 1 is the most straightforward for the stakeholder. Case 2 may be resolved by reviewing evaluation results with the stakeholders. If a weighted matrix evaluation method is used, inspecting the score and weighted score matrices may reveal patterns that are helpful and clear in the decision-making process. A review of weights and criteria may indicate that weights may be modified, which may resolve the overlap. Additional factors may be identified as criteria to resolve the overlap. If the overlap of weighted scores persists, the lowest cost alternative may be selected. Case 3 is the most difficult to resolve. A review of evaluation criteria, especially pass/fail and critical criteria, may indicate that no satisfactory alternative has been identified by the study. In this case, engineering judgment and discussions with the stakeholder shall be used to define additional alternatives or to accept a less than optimal alternative.

Figure 4.6-5 depicts typical utility curves used for sensitivity analysis.

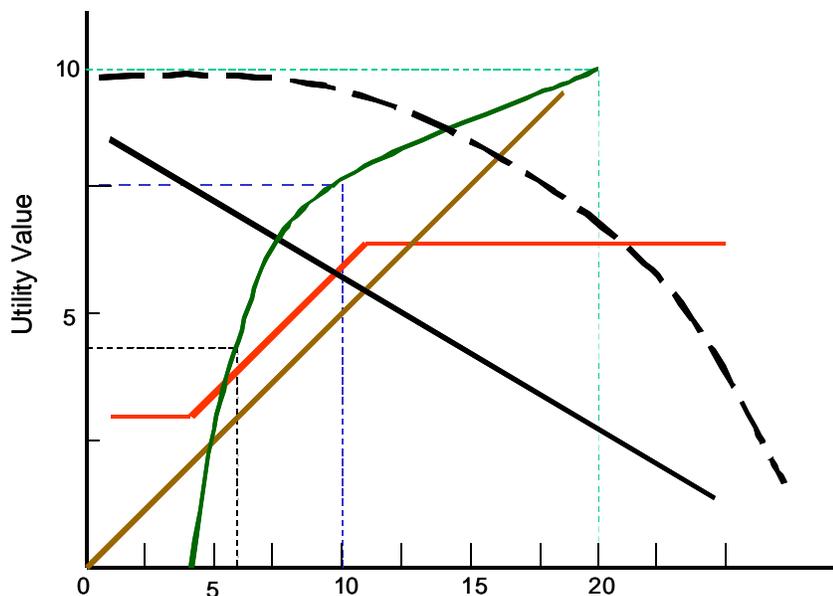


Figure 4.6-5. Example Utility Curves

#### 4.6.3.7 Task 7: Review Result and Form Conclusions

This part of the Trade Studies process typically presents one alternative that balances the Requirements and a "zero change" option for comparison. While the defined decision authority makes the final decision, a recommendation by the Trade Studies team is essential. All results shall be reviewed, any necessary additional data obtained, and evaluations and preliminary conclusions revised as needed. Any or all parts of the study may be repeated.

If the evaluation's intent is to select a product or service, it may be useful to review preliminary conclusions with vendors to ensure that no misunderstandings have occurred. Delaying such reviews until this phase of the evaluation avoids much of the risk of biasing the overall process.

When the evaluation is completed and deemed reliable, cost estimates for each alternative shall be prepared. Weighted scores for evaluation criteria are related to benefits associated with the evaluated alternative. The cost of an alternative divided by the total score for that alternative is a measure of the cost/benefits of that alternative.

At this point, the alternatives are now ordered based on the technical requirements and quantified impacts. It is recommended that changes from the baseline design technical performance and the decision criteria used during this evaluation be highlighted.

#### 4.6.4 Outputs of Trade Studies

The outputs of the Trade Studies process are a report with an executive summary and a design/manufacturing decision document.

##### 4.6.4.1 Trade Study Report

A Trade Study Report is prepared for each study. The report documents the study results and provides traceability to decisions made during the program's lifecycle. The report provides the traceability needed to substantiate design and configuration changes to the baseline design and also documents the decision-making process that selected one alternative over another. Additionally, it describes the effects of selecting a particular alternative among trades and clearly notes affected areas that were included in the Trade Studies assumptions, as well as affected areas that were not included in the associated trade. Once the report is completed, the Trade Studies leader is expected to coordinate the report with all affected team leaders before submitting it for approval and signature.

The Trade Study Report is prepared using a format appropriate for documenting and communicating the results, conclusions, risks, benefits, and recommendations to the decision maker. It is recommended that the format be standardized wherever possible to satisfy individual program needs. At a minimum, it is recommended that the following be included, but not limited to:

- Clear problem statement
- Identification of affected Requirements
- Ground rules and assumptions
- Decision criteria
- Resource requirements statement to accomplish the study
- Schedule to accomplish (proposed and actual)
- Evaluation of all potential solutions and screening matrix
- Comprehensive array of feasible alternatives
- Comparisons of alternatives using decision criteria
- Technical recommendation of the Trade Studies team
- Documentation of any decisions leading to the final technical recommendation

The following is a suggested report format. Each project may enhance the standard outline as needed by adding subsections and separately numbered items to the sections. Each project may also add sections and subsections for special topics and delete sections and subsections that are not applicable.

#### Table of Contents

- 1 Introduction

- 1.1 Scope
- 1.2 Applicable Documents
- 1.3 Definitions
- 2 Study Summary
- 3 Requirements Summary
- 4 Evaluation Criteria
  - 4.1 Evaluation Criteria and Scoring Method
  - 4.2 Evaluation Criteria and Changes During Study
- 5 Alternative Solutions
- 6 Results
  - 6.1 Evaluation Approach, Scores, and Analysis
  - 6.2 Conclusions

Appendices

List of Acronyms

References

#### **4.6.4.2 Design/Manufacture**

Once the Trade Study Report is approved, the design decision/manufacturing document is produced, outlining the impacts and actions necessary to implement the alternative recommended in the Trade Studies into the baseline configuration. In general, this document describes the rationale required to substantiate the change. The report then becomes an attachment to the design decision/manufacturing document and serves as the technical basis for the option to be implemented. The design decision document is submitted to the appropriate control authority to authorize implementation into the baseline configuration. The control authority is also required to maintain the report and the design/manufacturing decision document for the program's lifecycle.

#### **4.6.5 Trade Studies Tools**

##### **4.6.5.1 Quality Function Deployment**

QFD is a methodology used to ensure that the stakeholders' operational needs and requirements are gathered, interpreted, and deployed 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 Trade Studies tool that screens alternatives using weighted selection criteria. QFD is recommended for use whenever:

- Stakeholder requirements are vague, ambiguous, or self-contradictory
- Multiple disciplines are involved in the collection and interpretation of the requirements

- Multiple solutions are feasible with no clear choice
- Lack of an obvious feasible solution
- Cost and/or risk appear to be unacceptably high

QFD (see <http://www.shef.acu.uk/~ibberson/qfd.html>) requires teamwork among the multiple disciplines that make up a program/project team to address requirements from multiple perspectives. It is recommended that QFD involve the customer, representatives from the product development and support functions, and suppliers. It is also recommended that a team attempting to conduct a QFD exercise for the first time receive training before the start of the exercise and support from an experienced product-oriented QFD expert.

#### 4.6.5.2 Modeling and Simulation

Models and simulations are standard engineering tools that represent the key features of a system and the interactions of those features with each other and 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.

#### 4.6.6 Trade Studies Process Metrics

**Quality** may be measured by the degree to which the project objectives are satisfied, as noted in “Trade Studies Objectives” (subsection 4.6.1.1 above); objectives are satisfied when they may be numerically quantified (e.g., increase of payload capability). For imprecise objectives, project management may decide on a different type of assessment (e.g., yellow/red/green).

**Timeliness** may be measured by compliance with the schedule. It may be measured by when the decision support provided by the studies is available for the decision to be made.

**Resources** consumed to reach the required decision support level may identify efficiency, which may include labor hours, computer usage, and schedule time.

**Cycle time** may measure the duration from the creation of system alternatives to the delivery of the decision support products discussed in “Outputs of Trade Studies” (subsection 4.6.4 above).

**Process performance** is measured and recorded on a regular basis. Process users (teams or equivalent functions) accumulate the following metrics, at minimum, to evaluate the performance of this process:

- Percentage of studies performed in which none of the alternatives emerged conclusively as the best solution, thereby driving a decision based on other factors
- Percentage of studies in which the recommended alternative was not subsequently selected
- Percentage of planned discipline viewpoints, as defined by the study scope, that actively participated in conducting the Trade Studies

The decision maker completes the satisfaction assessment.

#### 4.6.7 References

1. Blanchard, Benjamin S. *System Engineering Management*. 2nd edition. New York, NY: John Wiley & Sons, Inc., 1998. (<http://www.wiley.com/>)
2. Blanchard, Benjamin S., and Fabrycky, Walter J. *Systems Engineering and Analysis*. 2nd edition. Englewood Cliffs, NJ: Prentice Hall, 1998.
3. Defense Acquisition University. *System Engineering Fundamentals*. Fort Belvoir, VA: Defense Acquisition University Press, 1999. <http://www.dau.mil/>
4. Shishko, Robert. *NASA Systems Engineering Handbook*. NASA SP-6105. Washington, DC: National Aeronautics and Space Administration, June 1995.
5. *Systems Engineering Handbook*. Version 2.0. Seattle, WA: International Council on Systems Engineering (INCOSE), 2000. (<http://www.incose.org/>)

## 4.7 Interface Management

### 4.7.1 Introduction to Interface Management

Interface Management, **which includes identification, definition, and control of interfaces, is 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.** Precisely defining interfaces early in the program is crucial to successful and timely system development. As the total system is decomposed into functional areas, functional interfaces between the areas are identified. These interfaces typically have functional data parameters with associated data requirements or mechanical, electrical, and space requirements. The Interface Requirements Document (IRD) contains performance, functional, and physical interface requirements. The Interface Management process enters the Acquisition Management Systems (AMS) process during Mission Analysis and continues through In-Service Management. Figure 4.7-1, the Process Based Management (PBM) chart, illustrates the essential elements of the Interface Management process. This figure lists the key inputs to initiate the step, providers, process steps, outputs, and customers of process outputs. It also shows the beginning and ending boundary steps and intermediate steps.

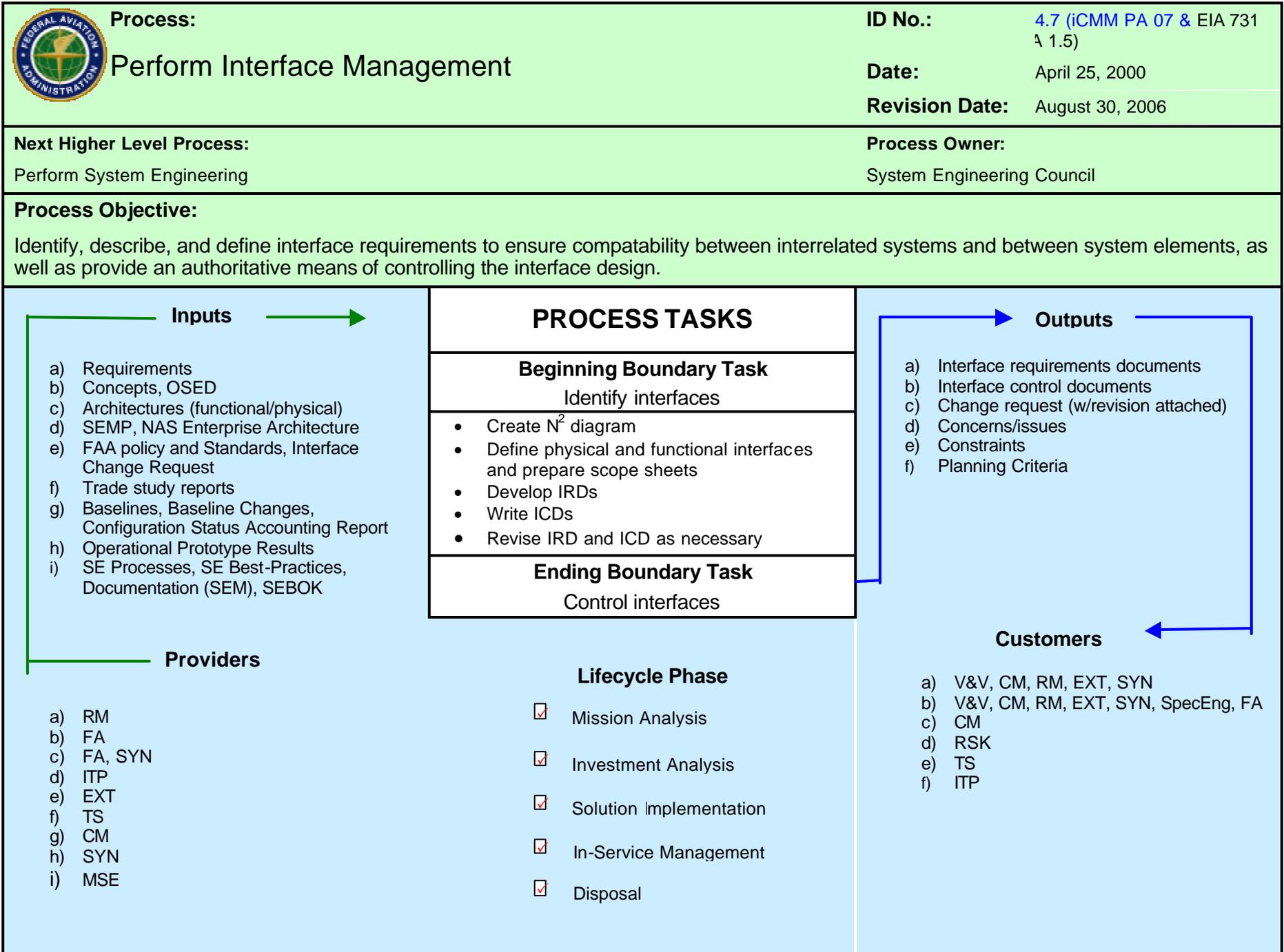


Figure 4.7-1. Interface Management Process-Based Management Chart  
 4.7-2

### 4.7.1.1 Interface Management Objectives

Interface Management identifies, describes, and defines interface requirements to ensure compatibility between interrelated systems and between system elements. It also provides an authoritative means of controlling the interface design.

The FAA uses the IRD to control interface requirements, while the Interface Control Document (ICD) controls interface design. These documents:

- Define and illustrate performance, physical, and functional characteristics in sufficient detail to ensure that all details on the interface can be determined solely from the information in the IRD/ICD
- Identify required interface data and monitor submission of this data
- Control the interface requirements and design to prevent any changes to characteristics that might affect compatibility with other systems and equipment
- Communicate coordinated interface requirements and design decisions as well as interface requirements/design changes to program participants

### 4.7.1.2 Types of Interfaces

**An interface is the performance, functional, and physical attributes required to exist at a common boundary.** Internal interfaces are within the defined system's boundary. External interfaces are with elements outside the defined system's boundary. The external/internal interface distinction relates to the level of ownership and the verification of the requirements associated with each interface. Examples of interface types that may be encountered appear in Table 4.7-1. Each element of the system shall be described functionally and physically. A functional description describes what the system is intended to do. It includes subsystem functions as they relate to and support the system function. Functional Analysis (Section 4.4) provides more information on this topic. A physical description describes the composition and organization of the tangible system elements. The level of detail varies with the system's maturity, size, and complexity, with the end objective being adequate understanding of the system configuration and operation.

Table 4.7-1. Examples of Interface Types

Interface Type	Interface Subtype	Examples
Functional	Mechanical	Vehicle operator increasing speed A printer converting electronic information into a printed document
Physical	Mechanical	Transmission of torque via a drive shaft Connection between computer communication port and the printer cable

Table 4.7-1. Examples of Interface Types—Continued

Interface Type	Interface Subtype	Examples
Functional	Control	A control signal sent from a flight control computer through a cable to an actuator (two interfaces) A human operator selecting a flight management system mode
Physical	Control	The connection between the flight control computer and the cabling A human operator's fingers adjusting a flight management system mode switch
Functional	Aerodynamic	Pilot notification of a stall Vortices impacting on an aircraft
Physical	Aerodynamic	A stall indicator on a wing A fairing designed to prevent vortices from impacting a control surface on an aircraft
Functional	Environmental (Natural or Induced)	Maximum/minimum temperature of radar electronics The amount of rain/snow that makes a sensor reading anomalous
Physical	Environmental (Natural or Induced)	Increased volume of mercury in thermometer reaching new markers on temperature scale Wind impacting radar antenna surface
Functional	Noise	Minimum decibels required for an alert to be heard
Physical	Noise	Sound waves impacting on person's ear drum
Functional	Space	Space required to perform maintenance
Physical	Space	Inserting hardware into existing rack
Functional	Data	A cockpit visual display to a pilot Weather Message Switching Center Replacement to Weather and Radar Processor (WARP) data transfer
Physical	Data	Light from cockpit visual display impacting on pilot's retina Weather data bits moving from communications cable to communications port on WARP
Functional	Electrical	Energy from a direct current (DC) power bus supplied to an anti-collision light A fan plugged into an alternating current (AC) outlet for current An electrical circuit opening a solenoid Shielding and grounding for coaxial cables

Table 4.7-1. Examples of Interface Types—Continued

Interface Type	Interface Subtype	Examples
Physical	Electrical	Energy from a DC power bus supplied to the cabling connected to the anti-collision light Electrical current moving from AC outlet to fan wire Current flowing through wiring
Functional	Hydraulic	Pressurized fluid supplying power to a flight control actuator A fuel system pulling fuel from a tank to the engine
Physical	Hydraulic	Pressurized fluid in a hydraulic line Connection of fuel line to fuel tank
Functional	Pneumatic	An adiabatic expansion cooling unit supplying cold air to an avionics bay An air compressor supplying pressurized air to an engine air turbine starter
Physical	Pneumatic	Pressurized air in an aircraft
Functional	Electro-magnetic	Radio frequency (RF) signals from a Very High Frequency Omni directional Range (VOR) A radar transmission
Physical	Electro-magnetic	RF signals from a VOR vibrating radio receiver Radio waves emitted from radio transmitter
Functional	Heating, Ventilating, and Air-Conditioning (HVAC)	Amount of heating and cooling required for a facility Circuit protective devices for equipment racks
Physical	HVAC	Thermocouple contacting sensor Circuit breaker connection to power line

The 5M and SHELL Models (Figures 4.7-2 and 4.7-3, respectively) depict the types of interface elements that are recommended for consideration within most systems.

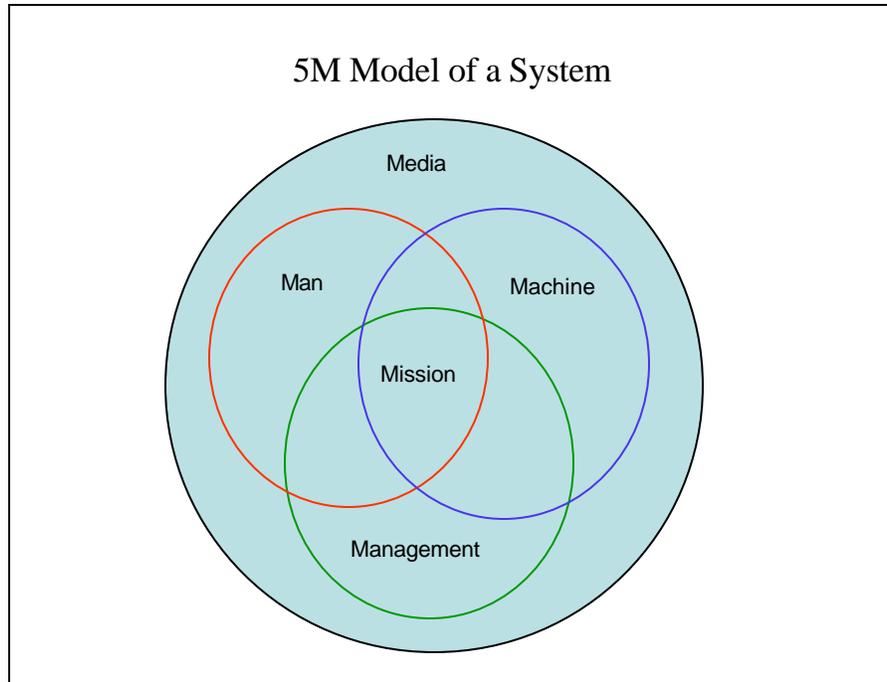
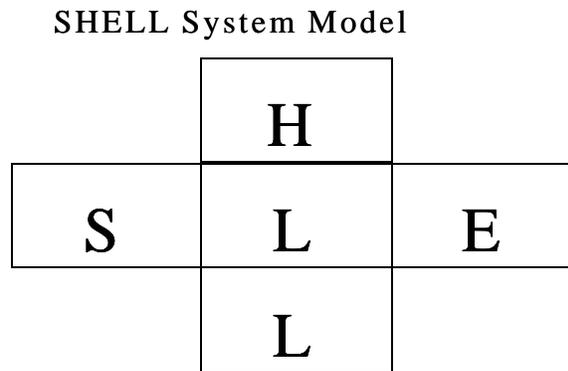


Figure 4.7-2. 5M Interface Model

The following is a description of the 5M Interface Model:

- **Mission:** the system's purpose or central function that brings together the other elements.
- **Man:** a system's human element. If a system requires humans for operation, maintenance, or installation, this element shall be considered in the system description.
- **Machine:** a system's hardware and software (including firmware) elements.
- **Management:** the procedures, policy, and regulations involved in operating, maintaining, installing, and decommissioning a system.
- **Media:** the environment in which a system shall be operated, maintained, and installed. This environment includes ambient and operational conditions. Ambient conditions are physical conditions involving temperature, humidity, lightning, electromagnetic effects, radiation, precipitation, and vibration. The operational environment consists of the conditions in which the mission or function is planned and carried out. Operational conditions are human-created conditions involving operations such as air traffic density, communication congestion, and workload. Part of the operational environment may be described by the type of operation (air traffic control, air carrier, general aviation); phase (ground taxiing, takeoff, approach, en route, transoceanic, landing); or rules governing the operation (Instrument Flight Rules versus Visual Flight Rules).

In the SHELL Model, the match or mismatch of the blocks (interface) is just as important as the characteristics described by the blocks themselves. These blocks may be rearranged to describe the system as required. A connection between two blocks indicates an interface between the elements.



S= Software (procedures, symbology, etc.)  
H= Hardware (machine)  
E= Environment (operational and ambient)  
L= Liveware (people)

Figure 4.7-3. SHELL Interface Model

#### 4.7.1.2.1 Functional Interfaces

Functional interfaces define the purpose of the interface. 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. Figure 4.7-4 illustrates this concept, where side A delivers some quantity (e.g., electrical power) to side B; at the same time, side B receives that quantity from side A. The two implied requirements are:

- Side A shall generate the quantity
- Side B shall provide a compatible response to the quantity that side A delivered

Interface requirements shall be expressed in verifiable terms. For example, as expressed in strict requirements terminology, "the [side A] subsystem shall deliver electrical power at 28 volts." In this example, the element of Side B is a fan. Thus, the requirement for side B might be as follows: "The fan [side B] shall provide impedance, power level and timeline, while using the 28-volt power supply of the electrical system Interface [Side A]. "The interface definition includes the data and/or control functions and the way these functions are represented.

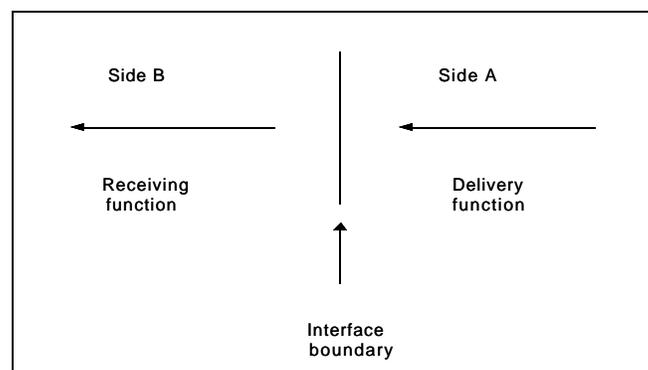


Figure 4.7-4. Example of a Simple Interface

#### 4.7.1.2.2 Physical Interfaces

Physical interfaces 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 environment.

#### 4.7.2 Inputs to Interface Management

Table 4.7-2 lists the inputs to initiate Interface Management, including both program/project- and product-related data. Many of these inputs are developed and refined through the continuous, iterative processes of other SE elements.

**Table 4.7-2. Interface Management Process Inputs**

Input	Reference
Concepts	Functional Analysis (Section 4.4)
Architecture	Synthesis (Section 4.5)
Requirements (preliminary Program Requirements (pPR)/final Program Requirements (fPR))	Requirements Management (Section 4.3)
International Standards	System Engineering in the Acquisition Management System Program Lifecycle (Chapter 3)
FAA Order/Standards	System Engineering in the Acquisition Management System Program Lifecycle (Chapter 3)
Functional Analysis	Functional Analysis (Section 4.4)
Draft SE input to Implementation Strategy and Planning (ISAP)	Integrated Technical Planning (Section 4.2)
Trade Study Report	Trade Studies (Section 4.6)
Engineering solution actions and impacts	Trade Studies (Section 4.6)
Interface Control Planning	Integrated Technical Planning (Section 4.2)
Interface Change Request	Interface Management (Section 4.7)

#### 4.7.3 Interface Management Process Steps

Interface Management is an SE element 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. It includes identification, definition, and control of interfaces. Table 4.7-3 outlines the process, and the subsequent subsections describe the process steps.

Table 4.7-3. Interface Management Process Inputs by Output Product

Inputs	Source Process	Initial AMS Phase	Output
Requirements Documents	Requirements Management (Section 4.3)	Mission Analysis	↓
Concepts	Functional Analysis (Section 4.4)	Mission Analysis	↓
Architecture	Synthesis (Section 4.5)	Mission Analysis	↓
Functional Interface List	Functional Analysis (Section 4.4)	Mission Analysis	↓
Operational System Environment Document (OSED)	Functional Analysis (Section 4.4)	Mission Analysis	↓
			<b>Scope Sheet</b>
FAA Policy	External	Investment Analysis	↓
Standards	External	Investment Analysis	↓
Draft Interface Control Planning section of System Engineering Management Plan (SEMP)	Integrated Technical Planning (Section 4.2)	Investment Analysis	↓
Requirements Documents (fPR)/Changes	Requirements Management (Section 4.3)	Investment Analysis	↓
System Requirements/Changes	Functional Analysis (Section 4.4) Synthesis (Section 4.5) Trade Studies (Section 4.6)	Investment Analysis	↓
Physical Architecture	Synthesis (Section 4.5)	Investment Analysis	↓
Trade Study Report	Trade Studies (Section 4.6)	Investment Analysis	↓
			<b>IRD</b>
IRD		Solution Implementation	↓
Interface Change Request	External	Solution Implementation	↓

Table 4.7-3. Interface Management Process Inputs by Output Product—Continued

Inputs	Source Process	Initial AMS Phase	Output
Physical Architecture	Synthesis (Section 4.5)	Solution Implementation	↓
Design Definition/Changes	Synthesis (Section 4.5)	Solution Implementation	↓
Final Interface Control Planning section of SEMP	Integrated Technical Planning (Section 4.2)	Solution Implementation	↓
			ICD
Interface Revision Proposal			Revised IRD/ICD

#### 4.7.3.1 Step 1: Identify Functional/Physical Interfaces

The first step in the Interface Management process is to identify the functional and physical interfaces, which is accomplished using N-squared ( $N^2$ ) diagrams. The functional interfaces are identified during the Mission Analysis phase, while the physical interfaces are identified during the Investment Analysis phase.

#### 4.7.3.2 Step 2: Create an $N^2$ Diagram

The  $N^2$  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. It applies to system interfaces and hardware and/or software interfaces. The “N” in an  $N^2$  chart is the number of entities for which relationships are shown. The  $N^2$  diagram requires the user to generate complete definitions of all the 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 the squares in the  $N \times N$  matrix represents the interface inputs and outputs. The presence of a blank square indicates that there is no interface between the respective functions. Interface information flows in a clockwise direction between functions (i.e., the symbol  $F1 \curvearrowright F2$  in Figure 4.7-5 indicates data flowing from function F1 to function F2; the symbol  $F2 \curvearrowleft F1$  indicates the feedback). That which passes across the interface is defined in the appropriate squares. The diagram is complete when each entity has been compared to all other entities. The  $N^2$  diagram shall be used in each successively lower level of decomposition. Figure 4.7-5 illustrates directional flow of interfaces between entities within an  $N^2$  diagram. (In this case, the entities are functions.)

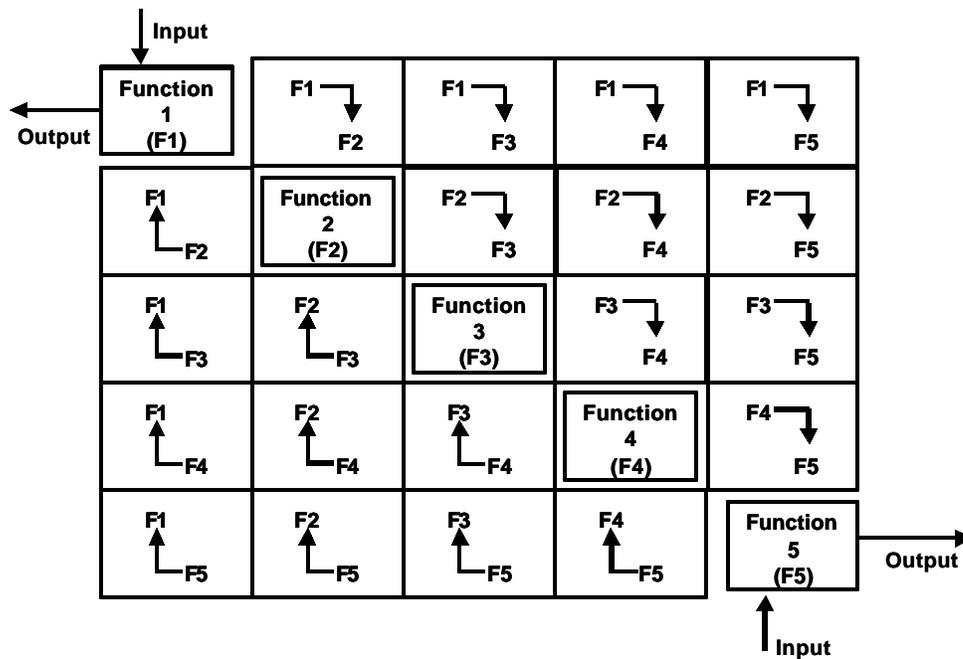


Figure 4.7-5. Generic  $N^2$  Diagram

In the example in Figure 4.7-5, N equals 5. Here, the five functions are listed on the diagonal. The arrows show the flow of data between functions. So if function 1 sends data to function 2, an X 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 an X would be placed in the first and third boxes to the immediate 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 an X 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 interfaces (functions). If there is no interface required between two functions, the corresponding square is left blank. Physical interfaces would be handled in the same manner.

In the example below (Figure 4.7-6), all data is acquired in function 1 from an external source. All acquired data is sent to function 2 for storage. However, some acquired data is sent to function 5 to be printed immediately. Therefore, there is an X in the first and fourth boxes to the right of function 1 showing this data flow. All data stored in function 2 can be retrieved by function 3. Function 3 sends the data to function 4 where it is reformatted and then sent to function 5 for printing. Thus, there is an X in the box to the immediate right of function 3 and 4. Since the system needs to save the reformatted data for possible retrieval and printing, there is an X in the box to the left of function 4 intersecting with function 2. However, since there may be a need for reformatted data to be printed at a later date, there is an X in the second box to the right of function 3, which shows the retrieval of reformatted data sent directly to the printer.

(If a functional architecture is provided, proceed directly to task 2). The following tasks are recommended for creating a functional  $N^2$  diagram:

**4.7.3.2.1 Task 1: Identify the Functional Interfaces Via an  $N^2$  Chart and Develop Functional Interface List**

- Create an  $N^2$  diagram that is  $N \times N$  square, where  $N$  is the number of system functions.
- Place the system functions on the diagram's diagonal axis.
- Moving across the diagram, fill in each square with any output, moving from function  $F_1$  to any of the succeeding functions. (Interfaces between functions flow in a clockwise direction.) If there are no outputs to a succeeding function, leave the square blank. (Characteristics of the entity (e.g., data, electrical power) passing between functions may be included in the box where the entity is identified.) Continue in this fashion until the upper half of the  $N^2$  diagram is populated.
- Moving down the diagram, fill in each square with any input, moving from function  $F_2$  to function  $F_1$ , from function  $F_3$  to function  $F_2$  or  $F_1$ , and so on with succeeding functions. If there are no outputs to a succeeding function, leave the square blank. Continue in this fashion until the lower half of the  $N^2$  diagram is populated.
- Conduct a peer review for completeness.

**4.7.3.2.2 Task 2: Develop a Functional Interface List From the Functional  $N^2$  Diagram**

The next action is to identify the physical interfaces via the  $N^2$  diagram during the Investment Analysis phase using the selected physical architecture.

**4.7.3.2.3 Task 3: Identify the Physical Interfaces Via an  $N^2$  Chart**

- Create an  $N^2$  diagram that is  $N \times N$  square, where  $N$  is the number of system elements.
- Place the system elements on the diagram's diagonal axis.
- Moving across the diagram, fill in each square with any output, moving from system  $S_1$  to any of the succeeding systems. (Interfaces between systems flow in a clockwise direction.) If there are no outputs to a succeeding system, leave the square blank. (Characteristics of the entity (e.g., data, electrical power) passing between systems may be included in the box where the entity is identified.) Continue in this fashion until the upper half of the  $N^2$  diagram is populated.
- Moving down the diagram, fill in each square with any input, moving from system 1 to system 2, from system 3 to system 2 or 1, and so on with succeeding systems. If there are no outputs to a succeeding system, leave the square blank. Continue in this fashion until the lower half of the  $N^2$  diagram is populated.
- Conduct a peer review for completeness.

**4.7.3.2.4 Task 4: Develop a Physical Interface List From the Physical N<sup>2</sup> Chart**

An example of an output from Task 3 appears in Figure 4.7-6. The N<sup>2</sup> diagram shall be taken down in successively lower levels to the hardware and software component levels. Another main function of the N<sup>2</sup> diagram in addition to interface identification is to pinpoint areas where conflicts may arise between systems and functions so that system integration occurring later in the development cycle proceeds efficiently.

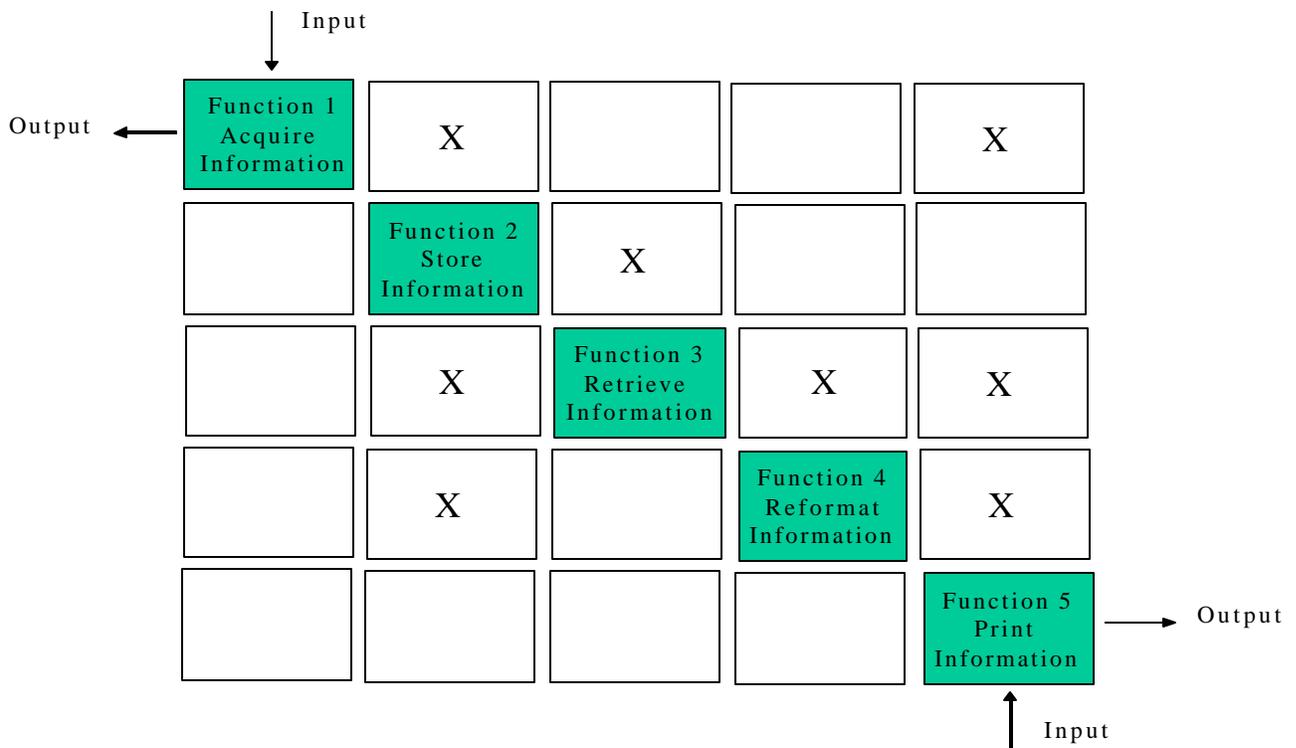


Figure 4.7-6. Example of a Simple N<sup>2</sup> Diagram

**4.7.3.3 Step 3: Define Functional and Physical Interfaces To Prepare Scope Sheets**

The third step in the Interface Management process is to define the functional and physical interfaces. This is achieved using scope sheets and IRDs. Scope sheets are used to develop the Interface Control planning section of the System Engineering Management Plan (SEMP). A summary of this information also appears in the Implementation Strategy and Planning (ISAP) (see Integrated Technical Planning (Section 4.2)). This Interface Control planning section defines a management system of interface controls to ensure physical and functional compatibility between interfacing system elements and between systems. This section also provides the means to identify and resolve interface incompatibilities and to determine the impact of interface design changes. Source material for the Interface Control planning section includes the concept documents, preliminary Program Requirements, and draft ISAP. Previously

developed N<sup>2</sup> diagrams are used to complete a scope sheet for each interface, which, in turn, is used to write the required IRDs.

The following tasks shall be performed when scope sheets are prepared:

- Review scope sheet format and example (Figures 4.7-7 and 4.7-8, respectively)
- Review functional and physical interface lists
- Prepare a scope sheet for each element in the diagonal, which corresponds to internal interfaces
- Review current program documents to determine required external interfaces
- Prepare scope sheets for all external interfaces
- Enter scope sheets into Configuration Management process (Section 4.11)

ICD NUMBER:		DATE INITIATED:	
REV:		DATE:	
ICD TITLE:			
PARTICIPANTS:			
SCOPE:			
EQUIPMENT RESPONSIBILITY:			
<b>INTERFACE LOCATION (INTERFACE BLOCK DIAGRAM)</b>			
PROGRAM REVIEWS and AUDITS:			
RELATED ICDs			
APPROVALS:			
Participant	Date:	Participant	Date:
IWG Secretariat	Date:	IWG Chairman	Date:

- Evaluate Scope Change Requests and update scope sheets as necessary

**Figure 4.7-7. Format of Scope Sheet for Interface Management**

ICD NUMBER: 25-DR010M REV: 1		DATE INITIATED: June 25, 3032 DATE: December 6, 3033	
ICD TITLE		Interface Control – Surveillance Radar Product Generator (RPG) – Weather System Processor (WSP) – Electrical Installation Envelope, Mechanical, Environmental, and Data	
PARTICIPANTS:		Green Electronics/Lockheed Martin	
SCOPE:		This IRD/ICD controls and documents all interface requirements for the RPG-to-WSP interface. Interface definition is described to the extent necessary to ensure compatibility of the RPG to WSP interfacing hardware when used with the specified constraints. The interface consists of mechanical installation of the WSP for cabling, mounting, environmental cooling, and data requirements. Mechanical interfaces include location, orientation, mounting provisions, and power supply. Envelope interfaces include installation, removal, connector, and cable clearances. Environmental interfaces include temperature and humidity constraints. The data interface includes Airport Surveillance Radar (ASR) 27 data (radio frequency, control, data, and timing signals) and WSP data (control and status signals).	
EQUIPMENT RESPONSIBILITY:		<ol style="list-style-type: none"> <li>Green Electronics — ASR-27 radar product generator</li> <li>Lockheed Martin — WSP module (hardware and software)</li> </ol>	
<b>INTERFACE LOCATION (INTERFACE BLOCK DIAGRAM)</b>			
PROGRAM REVIEWS and AUDITS:		Initial Requirement Review September 3032, System Requirements Review December 3032, Preliminary Design Review March 3033	
RELATED ICDs:			
APPROVALS:			
Raytheon	Date:	Lockheed Martin	Date:
IWG Secretariat	Date:	IWG Chairman	Date:

Figure 4.7-8. Example Scope Sheet

#### 4.7.3.4 Step 4: Develop Interface Requirements Documents

The next step in the Interface Management process is to develop IRDs, which, in turn, are used to develop ICDs. The designated custodian shall prepare the detailed IRD. FAA-STD-025 provides a checklist for IRD and ICD content. Commonly used FAA standards appear in Appendix G.

The following tasks shall be performed when IRDs are developed:

- Review the inputs listed in Table 4.7-2 (above)
- Prepare the detailed IRD in accordance with (IAW) FAA-STD-025
- Review the IRD for compliance with the final Program Requirements
- Coordinate the revised draft IRD with all affected organizations
- Enter the IRD into the Configuration Management process (Section 4.11)

#### 4.7.3.5 Step 5: Write Interface Control Documents

During this step, the detailed ICD/Interface Control Request is prepared and an analysis is performed to confirm completeness and accuracy of the interface definition. Often, this step is simplified through the use of an automated tool (see subsection 4.7.5 below). These documents shall be reviewed for compliance with the defined scope sheets and coordinated. A record of these actions shall be maintained. FAA-STD-025 provides a checklist for ICD content. The sequential tasks for this step are listed below.

- Review the inputs listed in Table 4.7-2
- Prepare the detailed ICD IAW FAA-STD-025
- Review the ICD for compliance with IRD
- Coordinate the revised draft ICD with all affected organizations
- Send the ICD to the Configuration Management process (Section 4.11)

#### 4.7.3.6 Step 6: Revise Interface Requirements Documents and Interface Control Documents

It may be necessary to request changes to the IRD/ICD as changes to Requirements or design definition occur. Following are the tasks for this step.

- Review the IRD for any required changes when design modifications occur or new requirements are added to the program requirements to determine if changes are required
- Review the ICD to determine if changes are also required
- Prepare the change request IAW FAA-STD-025 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

**Table 4.7-4. Interface Management Process Outputs and Destination SE Element**

Outputs	Destination SE Element
IRDs	Requirements Management (Section 4.3) Configuration Management (Section 4.11) Synthesis (Section 4.5) Validation and Verification (Section 4.12)
ICDs	External Requirements Management (Section 4.3) Functional Analysis (Section 4.4) Specialty Engineering (Section 4.8) Configuration Management (Section 4.11) Synthesis (Section 4.5) Validation and Verification (Section 4.12)
Interface Change Proposal (ICP)	Configuration Management (Section 4.11)

problems

- Description of resources and an estimate of the costs associated with implementing the change
- Statement of impact to system
- Provide change request to IWG, 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.
- Coordinate the draft IRD/ICD with all affected organizations
- Send Interface Change Request with revised IRD/ICD to the Configuration Management process (Section 4.11)
- Determine if IRD changes affect the program requirements and, if so, update them also

#### 4.7.4 Outputs of Interface Management

The outputs of the Interface Management process appear in Table 4.7-4. 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.

### 4.7.5 Interface Management Tools

The primary tool of Interface Management is a word processing tool. The FAA is developing a Web-based tool for development of IRDs and ICDs, which is currently being tested. It creates the document template for easy insertion of the appropriate interface data. For example, if a network IRD is selected, the document template only contains those paragraphs appropriate for a network IRD. Also, the tool automatically creates the Verification Requirements Traceability Matrix from the requirements inserted. Recommended interface requirements are inserted in the requirements database.

### 4.7.6 Interface Management Process Metrics

Table 4.7-5 lists the Interface Management process metrics.

**Table 4.7-5. Interface Management Process Metrics**

Quality Metrics	Cycle Time Metrics	Cost* Metrics
Scope Sheet in Compliance with Requirements (% "Yes")	Time from pPR to IRD Approval	Cost to implement IRDs
IRD in Compliance with Requirements (% "Yes")	Time from IRD Approval to ICD Release	Cost to implement ICDs
ICD/Interface Requirement Compliance with Interface Requirements (% "Yes")	Time from ICR Approval to Interface Requirement Release	Cost to implement ICRs
Design Compliance with ICD/Interface Requirement Requirements (% "Yes")		
Number of interfaces discovered after initial release of ICD		

\*Note: Cost is only direct program costs.

### 4.7.7 Terms and Definitions

**Interface:** The performance, functional, and physical attributes required to exist at a common boundary.

**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.

**IRD:** Document that provides the FAA interface requirements between two elements, including type of interface (e.g., electrical, pneumatic, hydraulic, etc.) and the interface characteristics (performance, functional, or physical). In its final form, the IRD is primary documentation of the interface requirements.

**ICD:** The “design” document that describes the detailed “as built” implementation of the requirements contained in the IRD. The ICD is one of the two primary products of the interface process and is usually developed by the vendor.

**Interface Control Planning Section of SEMP:** This section documents the formal management system of interface controls that ensures interface compatibility. Integrated Technical Planning (Section 4.2) provides detailed instructions on this topic.

**IWG:** The forum established through the SEMP and ISAP 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. The IWG shall consist of IWG chair, IRD/ICD custodian(s), and management personnel from associated teams. (Integrated Technical Planning (Section 4.2) provides detailed instructions on this topic.)

#### 4.7.8 References

1. Blanchard, Benjamin S. *System Engineering Management*. 2nd edition. New York, NY: John Wiley & Sons, 1998.
2. Buede, Dennis M. *The Engineering Design of Systems: Models and Methods*. New York, NY: John Wiley & Sons, 2000.
3. Defense Acquisition University. *System Engineering Fundamentals*. Ft. Belvoir, VA: Defense Acquisition University Press, 1999.
4. Grady, Jeffery O. *Systems Requirements Analysis*. New York, NY: McGraw-Hill, March 1999.
5. *NASA Systems Engineering Handbook*. SP-6105. Washington, DC: National Aeronautical and Space Administration, June 1995.
6. *Systems Engineering Capability Model*. EIA 731.1. Arlington, VA: Electronic Industries Alliance, December 1999.

## 4.8 Specialty Engineering

Specialty Engineering is a subset of System Engineering (SE) that defines and evaluates specific areas, features, and/or characteristics of a system. Specialty Engineering supplements the acquisition process by defining these characteristics and assessing their impact on the program. SE relies on specialty domain expertise to define and characterize specific requirements. SE's function in this process is to integrate the design engineer's activities and specialty engineer's activities, coordinate and open communication lines between the design engineer and specialty engineer, and focus the engineering effort on meeting the common goal of satisfying the customer—not on performing detailed Specialty Engineering work.

Engineers with specialized engineering skills conduct Specialty Engineering by primarily performing system analyses. These skill areas include System Safety Engineering (SSE); Reliability, Maintainability, and Availability (RMA); Human Factors Engineering; Electromagnetic Environmental Effects (E<sup>3</sup>); Quality Engineering; Information Security Engineering; and Hazardous Materials Management/Environmental Engineering. Engineers in these disciplines perform analyses throughout the system's lifecycle. The results are used to derive, validate, and verify requirements; evaluate system design progress and technical soundness; and manage risk. At a minimum, reports on the analysis results are available at standard design milestones, including the design, acquisition, and program reviews. When a supplier is involved, deliverables comply with contract requirements. Figure 4.8-1 shows the general process for performing Specialty Engineering, listing the key inputs to initiate the task, providers, process tasks, outputs required, and customers of process outputs.



**Process:**  
**Perform Specialty Engineering**

**ID No.:** 4.8  
**Date:** April 11, 2000  
**Revision Date:** August 30, 2006

**Next Higher Level Process:**  
 Perform System Engineering

**Process Owner:**  
 System Engineering Council

**Process Objective:**  
 Integrate specific system attributes and disciplines into the acquisition process and assess and confirm various system attributes.

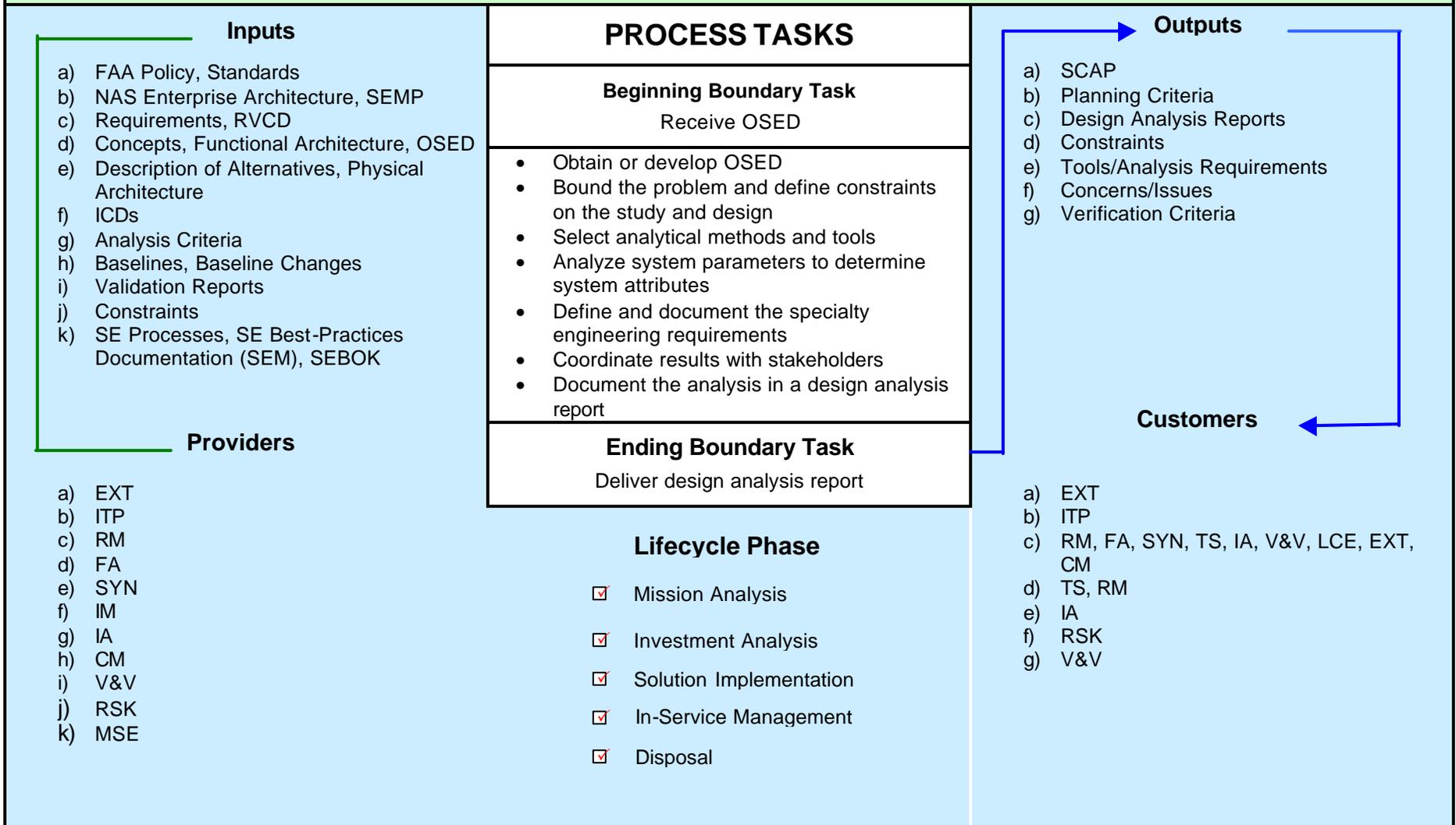


Figure 4.8-1. Specialty Engineering Process-Based Management Chart  
 4.8-2

## 4.8.0 Introductory Material

### 4.8.0.1 Introduction to Specialty Engineering

Engineers conduct Specialty Engineering throughout the system's lifecycle. Specialty Engineering analyses are conducted early to derive and validate requirements. In addition, the Specialty Engineering disciplines support the Functional Analysis (Section 4.4), Synthesis (Section 4.5), and Trade Studies (Section 4.6) efforts in selecting and designing solutions to requirements. Later in the lifecycle, after requirements at all levels are validated, these analyses provide support in verifying requirements by describing and assessing the characteristics of the design and/or operations. As early as possible in the lifecycle, the Specialty Engineering disciplines find and resolve potential program risk. Finding and controlling risk early assists decision makers in seeking the lowest possible cost and increases the probability of program success and operator acceptance of the product.

This section describes the functions, objectives, and products of the various Specialty Engineering disciplines.

#### 4.8.0.1.1 Description of Specialty Engineering Disciplines

Specialty Engineering analyses present characteristics of the system from a specific technical perspective. Table 4.8-1 gives a general description of the Specialty Engineering disciplines.

**Table 4.8-1. Specialty Engineering Disciplines**

Specialty Engineering Discipline	Description
SSE	Evaluation and management of the safety risk associated with a system using measures of safety risk identified in various hazard analyses, fault tree analyses, and safety risk assessments and in hazard tracking and control.
RMA	Quantitative and qualitative analyses of system attributes to optimize the RMA performance of a system within the program's operational and programmatic constraints throughout the system lifecycle. Quantitative assessments are probabilistic, mean, and/or distribution assessments; qualitative analyses are failure mode assessments.  Evaluation of the design's ability to meet operational readiness requirements through preventive and corrective maintenance.
Human Factors Engineering	Multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to: equipment, systems, facilities; procedures, jobs, environments; staffing; training; and Personnel and organizational management for safe, comfortable, and effective human performance.

Table 4.8-1. Specialty Engineering Disciplines—Continued

Specialty Engineering Discipline	Description
E <sup>3</sup>	<p>System analysis for susceptibility and/or vulnerability to electromagnetic fields or capability to generate such fields that might interfere with other systems, identify sources of interference, and implement methods for correction within the levels prescribed by law, program requirements, spectrum management, or recognized standards.</p> <p>E<sup>3</sup> consists of Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC).</p>
Quality Engineering	<p>An objective analysis of all planned and systematic activities to ensure that a product or service fulfills requirements and is of the highest quality.</p>
Information Security Engineering (ISE)	<p>Application of scientific and engineering principles to manage and control system security risk to the enterprise and its mission. Risk identification includes identifying system vulnerabilities and threats. ISE applies effective and suitable technical, procedural, physical, and administrative controls to mitigate these risks to an acceptable level. ISE combines control measures for prevention, detection, and recovery from security attacks that would compromise confidentiality, integrity, and/or availability of information technology assets (including information).</p>
Hazardous Materials Management/Environmental Engineering	<p>Determination of environmental impacts at deployment sites and during operations, including both environmental impacts on the system and system impacts on the environment during all phases of the product's life.</p>

In addition to resolving problems and defining requirements early, Specialty Engineering supplies information to the other SE functions, including Requirements Management (Section 4.3), Risk Management (Section 4.10), Configuration Management (Section 4.11), and Validation and Verification (Section 4.12). Table 4.8-2 highlights the effect that Specialty Engineering has on the other SE processes.

**Table 4.8-2. Major Effects of Specialty Engineering on Other System Engineering Processes**

Affected SE Process	How Affected
Integrated Technical Planning (Section 4.2)	The Integrated Technical Planning process feeds Specialty Engineering. Integrated Technical Planning produces the plans for Specialty Engineering, SE, and all other SE processes. The plans detail what is to be done, who is to do it, the standards of performance, and when each task is to be performed.
Requirements Management (Section 4.3)	The Requirements Management process both feeds and is fed by Specialty Engineering. The specialist describes the system in order to perform Specialty Engineering analyses. Requirements are a key component of any description, and they are an output of the Requirements Management process. Specialty Engineering studies often find characteristics that create a need for new or different requirements. Sometimes, the Specialty Engineering disciplines find areas of conflict between two or more requirements. In either case, the Specialty Engineering function develops the new or changed requirements, and these are an input to the Requirements Management process.
Functional Analysis (Section 4.4)	The Functional Analysis process both feeds and is fed by Specialty Engineering. To execute a Specialty Engineering analysis, the specialist shall have a thorough understanding of the system functions. This understanding is a result of performing a Functional Analysis of the system.
Interface Management (Section 4.7)	Specialty Engineering both feeds and is fed by Interface Management. The specialist describes the system to perform Specialty Engineering analyses. Interface Requirements Documents (IRD) are key components of any system description and are an output of the Interface Management process. Specialty Engineering studies often find characteristics that create a need for new or different interface requirements. Sometimes, the Specialty Engineering disciplines find areas of conflict between two or more interfaces. In either case, the Specialty Engineering function develops the new or changed requirements, which are inputs to the Interface Management process.

**Table 4.8-2. Major Effects of Specialty Engineering on Other System Engineering Processes—Continued**

Affected SE Process	How Affected
Risk Management (Section 4.10)	Specialty Engineering feeds the Risk Management process. Specialty Engineering studies and analyses find and assess potential problem areas of a design as early as possible. When a potential problem is found, the information becomes an input to the Risk Management process for risk mitigation and control.
Configuration Management (Section 4.11)	Specialty Engineering outputs are inputs to the Configuration Management process. In performing Specialty Engineering analyses, specialists may discover that additional or changed design features are required or that changes to operating, maintenance, or installation procedures are needed. When these discoveries occur, the proposed changes become inputs to the Configuration Management process.
Validation and Verification (Section 4.12)	<p>Specialty Engineering outputs feed the Validation and Verification process. Early in the program’s lifecycle, specialists use Specialty Engineering to validate requirements by comparing the requirements defined in early Specialty Engineering analyses to those defined in current/later analyses. If the Specialty Engineering analyses find a need for an existing requirement, then the requirement may be considered validated.</p> <p>Specialty Engineering feeds Verification Criteria to the Verification process. Specialists also use Specialty Engineering to verify requirements later in the system’s lifecycle, either by test or SE Assessment. Specialty Engineering is a form of assessment and may be used to demonstrate verification.</p>

**4.8.0.2 Inputs and Providers to Specialty Engineering**

Table 4.8-3 depicts the inputs needed to conduct Specialty Engineering analyses.

Table 4.8-3. Specialty Engineering Process Inputs

Process Input	Input Purpose/Description	From Process
FAA Policy and Standards	Policy and standards, such as the Acquisition Management System (AMS), define what is expected to be accomplished and how well it needs to be done.	AMS and FAA Orders
National Airspace System (NAS) Enterprise Architecture	The NAS Enterprise Architecture is the technical blueprint for modernizing the NAS and guides the Federal Aviation Administration (FAA) on what systems are planned for modernization.	Integrated Technical Planning (Section 4.2)
System Engineering Management Plan (SEMP)	The SEMP defines the plan for conducting SE in the AMS and a program.	Integrated Technical Planning (Section 4.2)
Requirements	<p>Requirements provide information about the system's required characteristics, specifications, performance, and requirements. They assist in developing the system description.</p> <p>System requirements are documented in the preliminary Program Requirements (pPR), the final Program Requirements (fPR), and system specification(s).</p>	Requirements Management (Section 4.3)
Requirements Verification Compliance Documents (RVCD)	The RVCD records the verification status of all requirements.	Requirements Management (Section 4.3)
Concepts	Concepts are captured in user-oriented documents that describe system functional characteristics for a proposed system from the user's viewpoint. It explains the existing system, current environment, users, interactions among users and the system, and organizational impacts. Concept documents communicate overall quantitative and qualitative system characteristics to the user, buyer, developer, and other organizational elements.	Functional Analysis (Section 4.4)

Table 4.8-3. Specialty Engineering Process Inputs—Continued

Process Input	Input Purpose/Description	From Process
Functional Architecture	<p>The Functional Architecture identifies, analyzes, and describes the functions of a system. It provides information required for a system description and assists in defining requirements.</p> <p>Functional Analysis is a System Engineering process that takes stakeholders' needs and translates them into a sequenced and traceable functional architecture.</p>	Functional Analysis (Section 4.4)
Operational Services and Environmental Description (OSED)	The OSED is a comprehensive, holistic system description that describes the services, environment, functions, and mechanizations that form a system's characteristics.	Functional Analysis (Section 4.4)
Description of Alternatives	Description of Alternatives conveys the various Physical Architectures being analyzed for implementation. When Trade Studies (Section 4.6) are performed, a number of alternatives shall be competitively evaluated.	Synthesis (Section 4.5)
Physical Architecture	Physical Architecture is a hierarchical arrangement of hardware and/or software components along with their associated interfaces that depicts the physical definition of the system.	Synthesis (Section 4.5)
Interface Control Document (ICD)	The ICD contains and documents the "as built" interface design derived from the IRD.	Interface Management (Section 4.7)
Analysis Criteria	Criteria for specialty engineering analyses specifically establish the degree of validation required for the analyses and associated tools, the methods for ensuring proper quality and range of data, and the level of documentation required.	Integrity of Analysis (Section 4.9)

Table 4.8-3. Specialty Engineering Process Inputs—Continued

Process Input	Input Purpose/Description	From Process
Baselines (i.e., Approved Baselines, Approved Baseline Changes, Updated Baselines)	When the requirements and design have matured sufficiently, they are baselined to facilitate management of the configuration.	Configuration Management (Section 4.11)
Validation Reports	Validation Reports document the results of the Validation effort. They report requirements that are validated and those that are considered nonconforming.	Validation (Section 4.12)
Constraints	Constraints are boundaries within which the system must remain. Risk mitigation plans often impose constraints that impact other areas of a program.	Risk Management (Section 4.10)
System Engineering Manual (SEM) Revisions	The SEM and its revisions are not direct inputs into the Specialty Engineering process. However, they do impact the actual conduct of the process. As the process is practiced, feedback from users may necessitate changes to the process. The SEM documents such changes.	System Engineering Process Management (Section 4.14)

#### 4.8.0.3 General Specialty Engineering Process Tasks

All Specialty Engineering disciplines follow a similar process during the conduct of associated analyses. The following subsections give general guidance on performing Specialty Engineering in the FAA. These processes, as shown above in Figure 4.8-1, are the following:

- Describe the system in physical and/or functional terms. The specialists must complete this task before beginning the analysis and should use existing system descriptions if they contain enough detail. If they don't, the specialists will have to generate a description, ensuring that it adheres to the guidance in Functional Analysis (Section 4.4) and Interface Management (Section 4.7).
- Bound the problem and define Constraints on the Specialty Engineering study and the design
- Select analytical methods and tools

- Analyze system parameters to determine specialty attributes that are specific to the views of the Specialty Engineering study
- Define or assess the Specialty Engineering Requirements
- Coordinate results with stakeholders
- Document the analysis results in a Design Analysis Report (DAR)

The following subsections detail the process tasks depicted in Figure 4.8-1.

#### **4.8.0.3.1 Task 1: Obtain or Develop an Operational Services and Environmental Description (OSED)**

The first task of the specialty engineer is to understand and describe the system at an appropriate level. The OSED is an excellent source for this information, since it is a system description that is developed in the Functional Analysis process (Section 4.4).

It is recommended that the specialty engineer use the existing descriptions to frame the Specialty Engineering analysis. However, sometimes the existing system descriptions lack sufficient detail. In these cases, the specialty engineer develops the system description; and, in doing so, shall comply with the guidance in Functional Analysis (Section 4.4).

Functional Analysis describes the desired behaviors of a system. These behaviors provide critical insight into how the system is intended to perform and, therefore, are a critical input to any Specialty Engineering analysis. To perform an assessment of a system, the engineer has to understand the functions of that system and be able to relate the specialties to these functions. Normally, Functional Analysis is completed before the Specialty Engineering process begins, and the specialty engineer only has to obtain and review the Functional Analysis and use it to enhance or complete the system description. In some cases—either because the engineers failed to perform it or because it is too early in the design process—the Functional Analysis is not available. In these cases, the specialty engineer shall refer to guidance in Functional Analysis and perform the Functional Analysis independently.

#### **4.8.0.3.2 Task 2: Bound the Problem and Define Constraints on the Study and Design**

Every system problem or analysis has breadth and depth. The breadth of a system analysis refers to the system boundaries. Boundaries limit the system to elements of the system model that affect or interact with each other in order to accomplish the central mission(s) or function. Depth refers to the level of detail in the description; this level varies inversely with the breadth of the system. For a system as broad as the NAS, the description and analysis are general in nature with little detail on individual components. On the other hand, a simple system, such as a valve in a landing gear design, includes significant detail to support the assessment.

Design Constraints play an important role in conducting analysis and the credibility of the results. It is essential to identify the Constraints before the analysis to account for their influence on the methods used and the alternatives chosen. As part of determining the Constraints, the engineer identifies the scope of the analysis, the ground rules, and assumptions. Identifying the customer(s) for the analysis is important with respect to defining the scope. The analysis may be subject to contractual restraints if it is a deliverable, and the engineer has to consider these restraints when defining the scope of the effort. The project schedule and budget may also impose limits on the analysis,

which may affect the assumptions and ground rules. The analysis team and the recipients of the report shall be aware of all the scope limitations, ground rules, assumptions, and guidelines that apply to the assessment and product design. The following sources are used to identify Constraints:

- Concepts defined via Functional Analysis (Section 4.4)
- Contract Statement of Work, including Work Breakdown Structure, and referenced standards and procedures
- Compliance documents that apply to the analysis methods and report
- Customer-specified requirements on cost, schedule, and product performance
- Management-imposed business goals and Constraints
- Functional, performance, and interface requirements derived from the design concept
- Functional, performance, and interface requirements imposed by use of commercially available or preexisting hardware and software
- Operational constraints imposed by the user
- Environmental constraints imposed by the physical and operational environment
- Constraints imposed by the production or Verification process (Section 4.12)
- Design constraints imposed by standard practices that are defined by the government or standards-setting bodies
- Federal, Department of Transportation, and FAA policies, standards, and guidelines

#### **4.8.0.3.3 Task 3: Select Analytic Methods and Tools**

To ensure Integrity of Analyses (Section 4.9), the engineer selects analytic methods and tools that meet the program phase requirements; the system analysis needs; and cost, schedule, and skill constraints. It is important to select methods and tools that match the analysis objectives within the resource limitations of the effort.

#### **4.8.0.3.4 Task 4: Analyze System Parameters To Determine System Attributes**

In this step, engineers use the methods and tools appropriate to the Specialty Engineering discipline to determine the attributes of the design. For some analyses, it is recommended that the results include programmatic attributes, such as cost and schedule impacts, as appropriate to the analysis. Table 4.8-4 lists the appropriate guidelines and handbooks for each Specialty Engineering discipline. The AMS FAA Acquisition System Toolset (FAST) often contains guidelines for these activities, such as the FAA System Safety Handbook (SSH) and the Safety Risk Management Guidance for System Acquisition (SRMGSA).

In addition, as part of this process, technical or peer reviews of the analysis and its results are conducted. The technical community conducts this independent evaluation before the Specialty Engineering DARs are submitted.

The results of Specialty Engineering analyses confirm design attributes necessary for acceptable product performance, cost, schedule, and risk. When an attribute is not confirmed, the analysis and/or the baseline shall be revised.

Revision may be implemented through changes in scope, ground rules, assumptions, and analytic methods. The analysis process is reactivated to determine an alternative result that is acceptable and valid. Alternatively, the results of the analysis may drive revision of the Requirements or design baseline. This revision is accomplished by preparing appropriate change proposal documentation for input to the Configuration Management process (Section 4.11).

**Table 4.8-4. Guidelines and Handbooks for Conducting Specialty Engineering**

Phase	Analysis	Guidelines and References
<b>Mission Analysis</b>	E <sup>3</sup> EMC requirements	FAST. (2000). Environment/Energy/Safety/Health. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a> FAST. (2000). Radio Spectrum Management. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Environmental Requirements Analysis	FAST. <sup>1</sup> Environment/Energy/Safety/Health. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Human Factors System (Mission) Analysis	FAST. Human Factors. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Human Factors Requirements and Functional Analysis	FAST. Human Factors. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Maintainability Requirements Analysis	FAST. Sustainment and Maintenance. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Operational Safety Assessment	FAST. System Safety Management. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a> FAA SSH <sup>2</sup> , Chapter 4 SRMGSA <sup>3</sup> , Chapters 3 and 4

<sup>1</sup> Federal Aviation Administration, Federal Acquisition System Tools (FAST), ATO, [On-line] Available: <http://fast.faa.gov>.

<sup>2</sup> U.S. Federal Aviation Administration, "FAA System Safety Handbook," ATO Safety Office (ATO-S), Washington, DC (2000).

<sup>3</sup> U.S. Federal Aviation Administration, "NAS Modernization System Safety Management Plan, ATO Safety Office (ATO-S), Washington, DC (2000).

Table 4.8-4. Guidelines and Handbooks for Conducting Specialty Engineering—  
 Continued

Phase	Analysis	Guidelines and References
	Information Security Engineering	Preliminary Risk Assessment, Guidance/Reference: FAA ISS Handbook 1370.82
<b>Investment Analysis</b>	Comparative Safety Assessment	FAST. System Safety Management. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a> FAA SSH, Chapter 4 SRMGSA
	EMC Control Plan	FAST. (2000). Environment/Energy/ Safety/Health. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a> FAST. (2000). Radio Spectrum Management. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Human Factors Program Plan	FAST. Human Factors. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Maintainability Plan	FAST. Sustainment and Maintenance. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Preliminary Hazard Analysis	FAST. System Safety Management. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a> FAA SSH, Chapter 8 SRMGSA
	Quality Engineering Plan	FAST. Quality Assurance. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Specialty Engineering Support of Trade Studies or Alternatives Analysis	FAST. Investment Analysis. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a> Synthesis of Alternatives (Section 4.5)
	System Safety Program Plan	FAST. System Safety Management. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a> FAA SSH, Chapter 5 SRMGSA
	Information Security Engineering	Updated Risk Assessment, Guidance/Reference: FAA ISS Handbook 1370.82

Table 4.8-4. Guidelines and Handbooks for Conducting Specialty Engineering—  
 Continued

Phase	Analysis	Guidelines and References
<b>Solution Implementation</b>	Environmental/ Hazardous Material Analysis	FAST. Environment/Energy/Safety/Health. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Failure Modes and Effects Analysis	FAST. System Safety Management. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a> FAA SSH, Chapter 8 SRMGSA
	Failure Modes and Effects Criticality Analysis	FAST. System Safety Management. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a> FAA SSH, Chapter 8 SRMGSA
	Hazard Tracking and Risk Resolution	FAST. System Safety Management. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a> FAA SSH, Chapter 3 SRMGSA
	Human Factors Demonstrations, Models, Simulations, and Mockups	FAST. Human Factors. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Human Factors Operator/Maintainer/ Supervisor Cognitive Task and Workload Analysis	FAST. Human Factors. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Human Factors Personnel, Staffing, and Training Analysis	FAST. Human Factors. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Human Factors Performance and Error Analysis	FAST. Human Factors. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Maintainability Analysis	FAST. Sustainment and Maintenance. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Maintainability Demonstration	FAST. Sustainment and Maintenance. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Maintainability Modeling	FAST. Sustainment and Maintenance. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Maintenance Task Analysis	FAST. Sustainment and Maintenance. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a>
	Operating and Support Hazard Analysis	FAST. System Safety Management. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a> FAA SSH, Chapter 8 SRMGSA

Table 4.8-4. Guidelines and Handbooks for Conducting Specialty Engineering—  
 Continued

Phase	Analysis	Guidelines and References
	Subsystem Hazard Analysis	FAST. System Safety Management. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a> FAA SSH, Chapter 8 SRMGSA
	System Hazard Analysis	FAST. System Safety Management. <a href="http://fast.faa.gov/">http://fast.faa.gov/</a> FAA SSH, Chapter 8 SRMGSA
	Information Security Engineering	Analysis supporting Certification and Authorization, Guidance/Reference: FAA ISS Handbook 1370.82

**4.8.0.3.5 Task 5: Define and Document Specialty Engineering Requirements**

The attributes developed in “Task 4: Analyze System Parameters To Determine System Attributes” (subsection 4.8.0.3.4) are used to define Specialty Engineering-related requirements. These requirements shall meet the standards for requirements definition and documentation described in Requirements Management (Section 4.3). In addition, these requirements shall be validated and verified, as described in Validation and Verification (Section 4.12).

**4.8.0.3.6 Task 6: Coordinate Results With Stakeholders**

The results of the Specialty Engineering process (particularly the DARs and Requirements) shall be coordinated with the project/program stakeholders in both formal and informal forums. The informal forums include peer reviews and working groups. The formal forums include Acquisition Reviews and Design Reviews, as described in Integrated Technical Planning (Section 4.2).

**4.8.0.3.7 Task 7: Document the Specialty Engineering Analysis in a Design Analysis Report**

The DAR is the primary output of any Specialty Engineering function. It documents the results—including the rationale—of the specific analysis. Each DAR shall contain the following results:

- Description of the system's special characteristics
- List of existing Requirements that were either validated or verified in the analysis
- Residual risks
- Candidate Requirements found as a result of the analysis

These DAR requirements are inputs to the Requirements Management process (Section 4.3) and shall be considered for inclusion in the preliminary Program Requirements (pPR) and the final Program Requirements (fPR). The rationale includes the scope, ground rules, assumptions, constraints, methods, and tools applicable to the analysis.

Specialty Engineering outputs are often used to validate and/or verify requirements. In addition, change proposal documentation is produced if the conclusions of the analysis call for a revision to the Requirements or design baseline. This revision is an input to the

Configuration Management process (Section 4.11) for authorization to change the baseline as the analysis indicates.

Requirements for contents and format may be applicable to the DAR as specified by the contract. Figure 4.8-2 is a sample outline of the DAR contents.

- 1.0 Executive Summary
- 2.0 Introduction
- 3.0 Summary of results
- 4.0 Summary of conclusions (including residual risks)
- 5.0 Recommendations (including mitigation)
- 6.0 System Description
  - 6.1 Summary
  - 6.2 Operational Services and Environment Description (OSED)
  - 6.3 Functional Analysis (if applicable)
  - 6.4 Requirements (if applicable)
- 7.0 Description of system special characteristics (detailed analysis worksheets or data)
- 8.0 List of candidate requirements
- 9.0 List of requirements that were validated and/or verified with rationale
- 10.0 Analysis methodology with rationale

**Figure 4.8-2. Sample Outline of a Design Analysis Report**

#### **4.8.0.4 Outputs of Specialty Engineering**

These are the Specialty Engineering outputs, which are described in subsequent subsections.

- Security Certification and Authorization Package
- Planning Criteria
- DARs (specific to the Specialty Engineering study)
- Constraints
- Tools/Analysis Requirements
- Concerns and Issues
- Verification Criteria

##### **4.8.0.4.1 Security Certification and Authorization Package**

For certification information, see subsection 4.8.6.

#### **4.8.0.4.2 Planning Criteria**

Any Planning Criteria needed to perform Specialty Engineering throughout the remainder of the program's lifecycle is provided to the Integrated Technical Planning process (Section 4.2).

#### **4.8.0.4.3 Design Analysis Report**

The DAR documents and reports the methods and results of the Specialty Engineering analyses. Figure 4.8-2 (above) provides a sample outline of a DAR. In performing an analysis, the specialty engineer typically defines, refines, or validates requirements. Occasionally, the specialist discovers system characteristics that are not adequately specified in the existing requirements or specification documents. In these cases, the specialist defines or modifies those requirements in the DAR to be consistent with the specialist's area of expertise and the requirements standards described in Requirements Management (Section 4.3).

#### **4.8.0.4.4 Constraints**

Constraints for performing Specialty Engineering throughout the remainder of the program's lifecycle need to be provided to the Trade Studies process (Section 4.6).

#### **4.8.0.4.5 Tools/Analysis Requirements**

Tools/Analysis Requirements for performing Specialty Engineering throughout the remainder of the program's lifecycle need to be provided to the Integrity of Analyses process (Section 4.9).

#### **4.8.0.4.6 Concerns and Issues**

Appendix D contains guidance on Concerns and Issues as a product of Specialty Engineering.

#### **4.8.0.4.7 Verification Criteria**

The specialist may be asked to define specific verification requirements, as described in "Step 3: Develop Verification Approach" in Section 4.12 (subsection 4.12.2.5.2.2.3). The Verification Criteria or requirements are added to the Verification Requirements Traceability Matrix (VRTM).

#### **4.8.0.5 Specialty Engineering Tools**

Each Specialty Engineering discipline often uses unique Specialty Engineering tools. They include databases, drawing tools, requirements and Functional Analysis tools, word and document processors, and spreadsheets. Selection of specific tools depends on criteria established by the particular program. These tools are identified and controlled as documented in appropriate program planning documents.

#### **4.8.0.6 Specialty Engineering Process Metrics**

The extent of progress being made in completing the Specialty Engineering analyses, as compared with the program's plans for conducting such analyses, is a measure of the degree to which these analyses are being effectively managed. The effectiveness of Specialty Engineering analyses may be measured by the extent of rework of analyses or incompatibility of analyses with measured performance, indicating that the analyses are reaching inaccurate conclusions.

Additional candidate metrics that measure the overall process and products of Specialty Engineering include:

- Percent of validated assumptions pertaining to the DAR
- Percent of validated Specialty Engineering requirements recommended in the DAR
- Percent of verified Specialty Engineering requirements recommended in the DAR
- Percent of open concerns and issues that have been identified as a result of the Specialty Engineering process

### 4.8.1 System Safety Engineering

System Safety Engineering (SSE) is a Specialty Engineering discipline within SE. It is recommended that system/safety engineers and program managers refer to the FAA’s Safety Management System (SMS) Manual, the Safety Risk Management Guidance for System Acquisition (SRMGSA), and the FAA’s System Safety Handbook (SSH) for detailed information for planning and conducting SSE. The following paragraphs describe how system safety is integrated into a system’s overall SE.

#### 4.8.1.1 What Is System Safety Engineering?

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 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 (<http://fast.faa.gov/toolsets/SafMgmt/indexstart.htm>) provides more information on this topic.

As illustrated in Figure 4.8.1-1, the SSE process is a closed-loop method of Risk Management (Section 4.10).

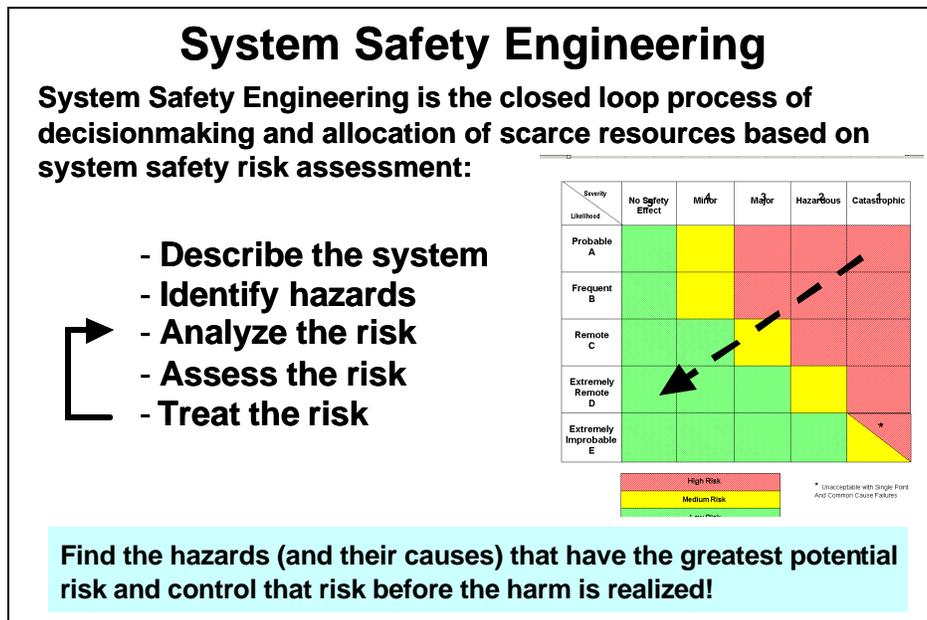


Figure 4.8.1-1. Closed-Loop Nature of System Safety Engineering

The following documents describe how SSE is conducted in the AMS:

- Chapter 4 of the FAA’s SMS Manual
- Chapter 4 of the SRMGSA (<http://fast.faa.gov/toolsets/SafMgmt/indexstart.htm>)
- Chapter 8 of the FAA SSH (<http://fast.faa.gov/toolsets/SafMgmt/indexstart.htm>)

Figure 4.8.1-2 shows what safety analyses are performed relative to the phases of the AMS. The analyses are timed to best support the phased needs and decisions in the overall AMS process.

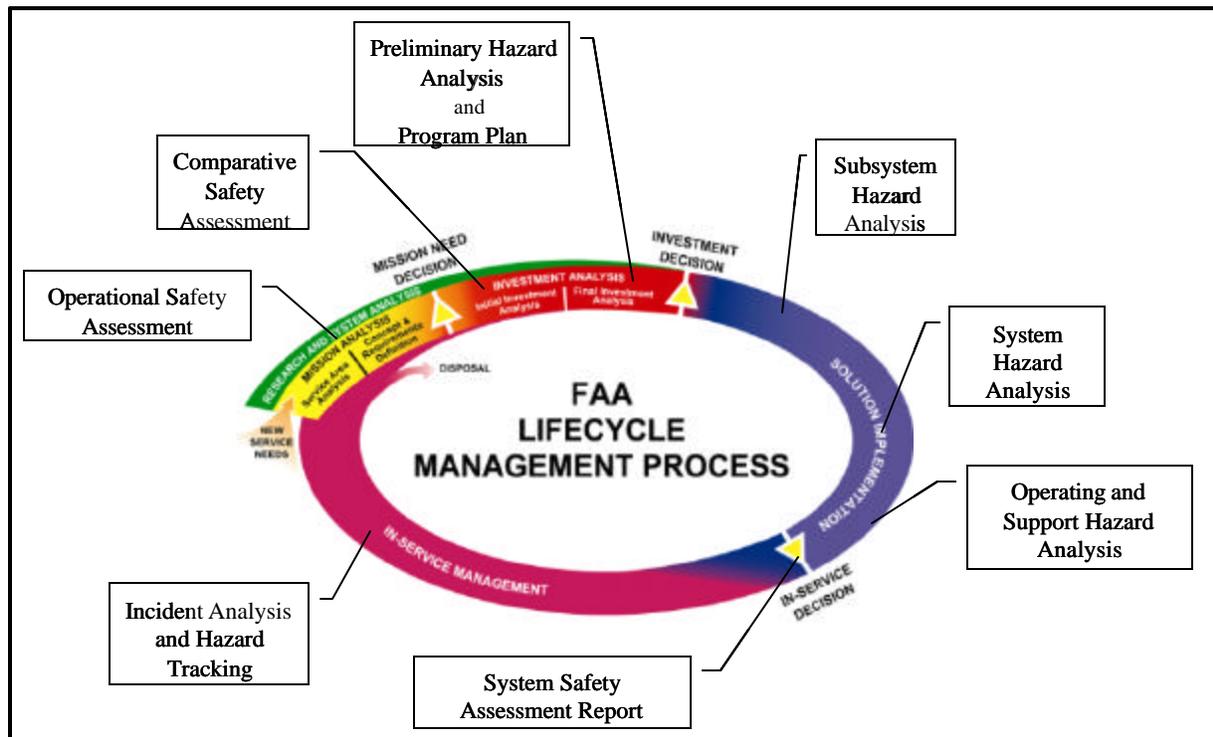


Figure 4.8.1-2. Types of Safety Hazard Analyses and Their Relative Position in the Acquisition Management System

#### 4.8.1.2 Why Perform System Safety Engineering?

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.** The FAA’s primary role is to ensure the safety of the NAS. Thus, the FAA has issued FAA Order 8040.4, which directs all FAA organizations to employ safety risk management in decision making. The safety risk management sections of the FAA’s 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 brief the system safety program status at all decision points and investment reviews. The SSH, the SRMGSA, and the AMS provide more information on this subject (<http://fast.faa.gov/toolsets/SafMgmt/IndexStart.htm>).
- **Reduce total cost of development.** SSE reduces cost and improves system integration and SE overall. SSE looks for programmatic risks that may impact system performance, schedule, and costs and finds problems early. As Figure 4.8.1-3 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 4.8.1-4).

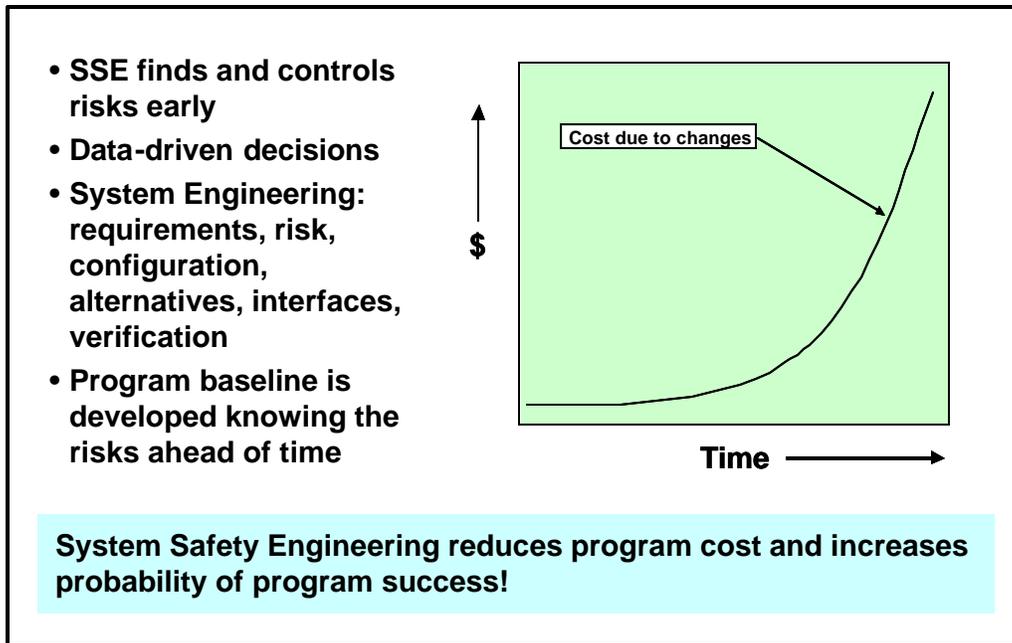


Figure 4.8.1-3. Benefits of System Safety Engineering

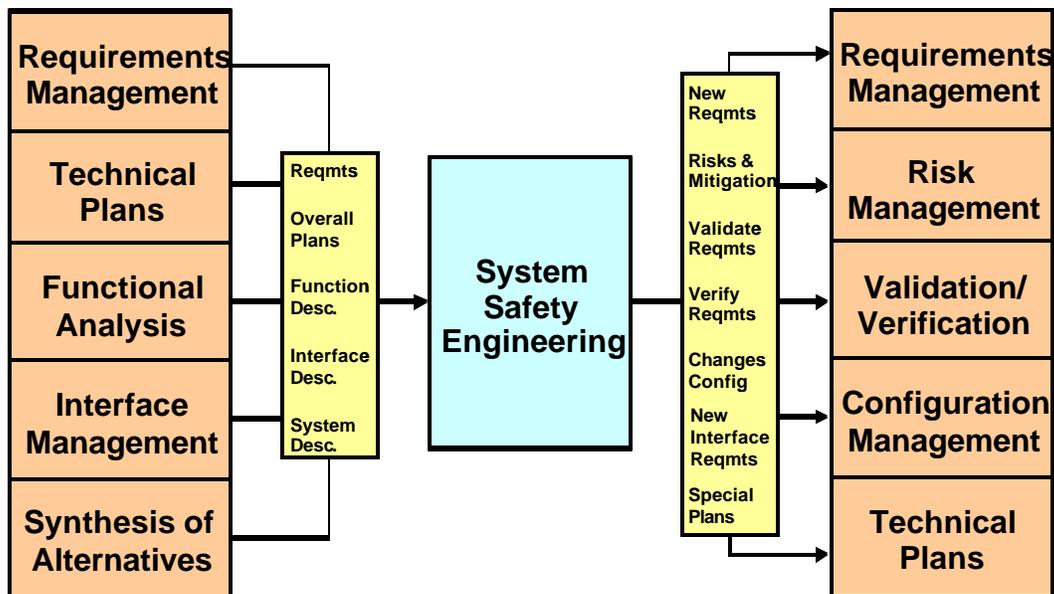


Figure 4.8.1-4. System Safety Engineering's Relationship to Other System Engineering Processes

#### 4.8.1.2.1 System Safety Engineering Process Tasks

SSE follows the process tasks outlined in "General Specialty Engineering Process Tasks" (subsection 4.8.0.3). These general tasks correlate directly with the specific SSE tasks in Table 4.8.1-1 and, as previously stated, appear in the FAA's SMS Manual and SSH and the NAS SSMP.

Table 4.8.1-1. General Specialty Engineering Tasks Correlated to SSE Tasks

General Specialty Engineering Process Tasks	Specific SSE Process Tasks
Obtain or develop an OSED	<b>Describe the system</b> 1. Describe the system or operation that is being added or changed 2. Plan the safety risk-management effort (define scope and objectives; identify stakeholders)
Bound the problem and define Constraints on the study and design	
Select analytical methods and tools	
Analyze system parameters to determine system attributes	<b>Identify hazards</b> 3. Identify the hazards 4. Identify hazard causes
	<b>Analyze the risk</b> 5. Assess the risk of the hazards (i.e., severity and likelihood) 6. Analyze existing controls
	<b>Assess the risk</b> 7. Rank hazards 8. Prioritize hazards
Define and document Specialty Engineering requirements	<b>Treat the risk</b> 9. Define risk-management strategies 10. Select risk-management strategies 11. Implement risk-control strategies 12. Verify control strategies through monitoring and tracking
Coordinate results with stakeholders	
Document the Specialty Engineering analysis in a DAR	

### 4.8.1.3 System Safety Engineering Outputs and Products

The following products are SSE outputs.

#### 4.8.1.3.1 Program Planning

Each program has to have a Program Safety Plan (PSP) per the SRMGSA, 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 vendor's or contractor's System Safety Program Plan (SSPP). The FAA SSH, Chapter 5 (<http://fast.faa.gov/toolsets/SafMgmt/indexstart.htm>), also provides guidance on this topic.

4.8.1.3.2 Analysis Products

Table 4.8.1-2 lists the SSE products and detailed directions on how to develop them.

Table 4.8.1-2. Products of System Safety Engineering

System Safety Process Products	How To Reference
Operational Safety Assessment (OSA)	FAA SSH, Chapters 2 and 4 ( <a href="http://fast.faa.gov/toolsets/SafMgmt/indexstart.htm">http://fast.faa.gov/toolsets/SafMgmt/indexstart.htm</a> ) SRMGSA, Section 5.2.1 ( <a href="http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.1">http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.1</a> )
Comparative Safety Assessment (CSA)	FAA SSH, Chapters 2 and 4 SRMGSA, Section 5.2.2 ( <a href="http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.2">http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.2</a> )
Preliminary Hazard Analysis (PHA)	FAA SSH, Chapter 8 NAS SSMP, Section 5.2.3 ( <a href="http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.3">http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.3</a> )
Integrated Safety Plan (ISP)	SSMP, Section 5.2.4 ( <a href="http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.4">http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.4</a> )
System Safety Program Plan (SSPP)	FAA SSH, Chapter 5 SRMGSA, Section 5.2.4 ( <a href="http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.4">http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.4</a> )
Subsystem Hazard Analysis (SSHA)	FAA SSH, Chapter 8 SRMGSA, Section 5.2.5 ( <a href="http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.5">http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.5</a> )

Table 4.8.1-2. Products of System Safety Engineering—Continued

System Safety Process Products	How To Reference
System Hazard Analysis (SHA)	FAA SSH, Chapter 8 SRMGSA, Section 5.2.6 ( <a href="http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.6">http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.6</a> )
Operating and Support Hazard Analysis (O&SHA)	FAA SSH, Chapter 8 SRMGSA, Section 5.2.7 ( <a href="http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.7">http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.7</a> )
Health Hazard Assessment (HHA)	FAA SSH, Chapter 8 SRMGSA, Section 5.2.8 ( <a href="http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.8">http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.8</a> )
System Safety Assessment Report (SSAR)	SRMGSA, Section 5.2.10 ( <a href="http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.10">http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.10</a> )
Hazard Tracking Risk Resolution System (HTRR)	FAA SSH, Section 2.2.3 SRMGSA, Section 5.2.11 ( <a href="http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.11">http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.11</a> )
Safety Requirements Verification Table (SRVT)	SRMGSA, Section 5.2.12 ( <a href="http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.12">http://fast.faa.gov/toolsets/SafMgmt/section5.htm#5.2.12</a> )

## 4.8.2 Reliability, Maintainability, and Availability Engineering

This section provides guidance to facilitate, manage, and coordinate Reliability, Maintainability, and Availability (RMA) efforts, which ensure operationally acceptable RMA characteristics in fielded systems.

### 4.8.2.1 What Is RMA Engineering?

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. These engineering and related management tools are used to identify, evaluate, and control RMA characteristics associated with a system. Thus, RMA Engineering primarily minimizes the probability of system failure and any potential losses stemming from such failure. RMA accomplishes this by establishing RMA requirements, assessing system RMA attributes, and analyzing solutions developed to meet established RMA requirements within realistic cost constraints.

#### 4.8.2.1.1 RMA Detailed Definitions

The following detailed RMA definitions provide background and context for the subsequent RMA Engineering discussions:

- *Reliability* quantifies a system's ability to perform without failure
- *Maintainability* quantifies a system's ability to recover from failure
- *Availability* quantifies a system's ability to perform when needed

##### 4.8.2.1.1.1 Reliability

Reliability is the 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 Failures (MTBF). Quantitatively, this translates to the probability that a system or constituent piece may perform a required function under specific conditions for a stated period of time. The formula in Equation 1 calculates Reliability.

$$R(T_2 - T_1) = e^{-\int_{T_1}^{T_2} h(t) dt}$$

Equation 1. Reliability Formula

where:

- $R(T_2 - T_1)$  is the *Reliability*, or probability that the system will not fail during the interval from time  $T_1$  to  $T_2$ , assuming no failure at  $T_2$ , and
- $h(t)$  is the *Hazard Rate*, or average rate of failure per hour experienced over specified small time intervals (e.g., 1 hour)

Whereas hazard rates are measured over small intervals of time (e.g., 1-hour periods), another useful metric for reliability characterization is the *Failure Rate*, which is the average hazard rate per hour, averaged over a given period of operating time, as follows:

$$I(T_2 - T_1) = \frac{\int_{T_1}^{T_2} h(t) dt}{T_2 - T_1}$$

where:

- $\lambda(T_2 - T_1)$  is the failure rate from time  $T_1$  to  $T_2$

Another reliability parameter is the *Mean Time To Failure* (MTTF), which is 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. It is related to the failure rate of the system as follows:

$$MTTF(T_2 - T_1) = \frac{1}{I(T_2 - T_1)}$$

The above equations show that the three fundamental parameters defined include time-based dependencies. This implies nonlinear complexities when component reliability values are aggregated to characterize the reliability of the system they comprise. However, during the operational phase of deployed system, hazard rates tend to maintain a constant value, especially at the component level. This assumption allows use of the following simplified relationships and parameters:

$$I(T) = h(t) = I$$

that is, the hazard rate is equal to the failure rate, which is constant over time, and,

$$MTBF = MTTF = \frac{1}{I}$$

where MTBF is the Mean Time Between Failures, the basic measure of reliability for repairable systems or constituent pieces with time-constant hazard rates. MTBF is the mean number of life units during which all parts of the system or constituent pieces perform within their specified limits, during a particular measurement interval under stated conditions. Equation 2 calculates MTBF.

$$MTBF = \frac{T}{F}$$

Equation 2. MTBF Formula

where:

- $T$  is the duration of the measurement interval
- $F$  is the number of failures that occurred during the measurement interval

#### 4.8.2.1.1.2 Maintainability

Maintainability is the measure of the ability of a failed system or constituent piece to be restored to full operational status. It is generally characterized by the Mean Time To Restore (MTTR), which is the average total elapsed time from initial failure to resumption of operation. MTTR includes *all* downtime, including the average time to obtain spares and appropriate personnel to begin the repair (i.e., Mean Logistic Delay Time) and the time to repair and restore the system. It is expressed as the sum of the logistic delay, corrective diagnosis, and maintenance times, divided by the total number of failures of a system or constituent piece. (see Equation 3). MTTR is usually expressed in hours.

$$MTTR = \frac{\sum_{t=1}^{F_T} \text{LogisticDelay}_t + \text{Diagnosis}_t + \text{Maintenance}_t}{F_T}$$

Equation 3. MTTR Formula

where:

- $t$  is an integer representing an occurrence requiring corrective diagnosis and associated corrective maintenance
- $T$  is the duration of the measurement interval
- $F_T$  is the number of failures that occurred during the measurement interval
- $\text{LogisticDelay}_t$  is the time to gather spare parts, equipment, and appropriate personnel to begin the repair
- $\text{Diagnosis}_t$  is the time to perform corrective diagnosis
- $\text{Maintenance}_t$  is the time to perform corrective maintenance

Maintainability requirements generally pertain to inherent characteristics of the system design (e.g., the ability to detect, isolate, access, and replace the failed component). In addition, a key characteristic to be addressed is any maintenance agreement for the system (e.g., warranties, incentives, and level of maintenance involved). System characteristics are generally fixed for commercial-off-the-shelf (COTS) components but may be specified, provided they do not conflict with the FAA's preference to employ COTS-based solutions whenever feasible.

### 4.8.2.1.1.3 Availability

Availability is 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. From a service perspective, availability is the percentage of time within any given interval that the service is provided to the expected level of performance specified within the target domain. Availability is appropriate as a top-level operational requirement because it is a quantitative and consistent way of summarizing the need for continuity of NAS services. Use of availability requirements may facilitate comparison and assessment of architectural alternatives. Availability is also useful as a performance metric for operational systems. Measured as a probability, availability may be defined in several ways, which allows a variety of issues to be addressed appropriately, including:

- **Inherent Availability.** This availability strictly represents the theoretical maximum availability based only on reliability (MTBF) and maintainability (MTTR). It only includes availability of the hardware components of the system. These are the only components that you can predict. Any other effects have to be measured and are included in other availability measures. The availability requirement associated with the highest criticality service supplied by the system is used to specify the inherent availability of the system. The only purpose for imposing an inherent availability requirement is to ensure that proposed constituent pieces of the system are theoretically capable of meeting a higher level requirement, based on the reliability and maintainability characteristics of these constituent pieces and the redundancy provided.
- **Equipment and Service Availability.** This availability includes all causes of unscheduled downtime. It takes into account additional downtime incurred during the failover to redundant systems or downtime incurred by other practical issues associated with unscheduled outages.
- **Operational Availability.** This availability includes scheduled and unscheduled downtime. Unlike inherent availability, operational availability includes the effects of scheduled downtime, shortages of spares, unavailable service personnel, or poorly trained service personnel. For systems or constituent pieces employing redundant elements, perfect recovery is assumed. Downtime occurs only if multiple failures within a common timeframe result in outages of the system or one or more of its pieces to the extent that the need for redundant resources exceeds the level of redundancy provided.

### 4.8.2.2 Why Perform RMA Engineering?

RMA directly impact both operational capability and lifecycle costs and, therefore, are important considerations in any system engineering effort. A system's ability to successfully fulfill its mission need directly depends on its ability to perform the required function under specific conditions for a given period of time without failure (reliability). Likewise, a system's operational success also depends on its ability to recover from a failure in a timely and efficient manner (maintainability). Operational success also depends on the system being ready to accomplish its mission as needed (availability). Operational and support costs for a system are predominant variables of its overall lifecycle cost. A major driver for these costs is the quality of a system's RMA characteristics. For example, redundancy is the simplest way to increase availability, although the overall system lifecycle cost increases.

To effectively and successfully coordinate RMA Engineering efforts and optimize the quality of a system's RMA characteristics, one must focus on the following objectives throughout the lifecycle of a system:

- Identify all system RMA functions, including all operational and maintenance support drivers; comprehensively incorporate RMA principles into the system requirements and design; and minimize and control the system lifecycle costs
- Measure, predict, assess, and report system trends throughout the system's lifecycle to continuously ascertain that RMA performance requirements are being met
- Achieve RMA performance objectives at all system levels
- Emphasize continuous RMA improvement

#### **4.8.2.2.1 RMA Issues**

In specifying availability, the steady state constant value (which characterizes the system availability in the long term) is not sufficient as the primary RMA requirement because it implies a tradeoff between reliability and maintainability. For example, a 1-hour interruption of a critical service that occurs annually is apparently equivalent to 240 15-second interruptions of the same service, since both scenarios provide the same availability. However, short interruptions lasting seconds are less likely to affect air traffic control operations than long interruptions lasting 1 hour or more, which may have a significant impact on traffic flow and operational safety. To address this issue, use both a steady state constant value and a dynamic expression of the system availability  $[A(T)]$ , which describes the proportion of time that a system is expected to be fully functional over a specified time interval  $T$  (e.g., for the next 100 hours of operation). This metric can be used to assess availability performance over smaller bounds of time to hone in on the expectation for short interruptions in service.

In addition, availability cannot be measured as an instantaneous parameter value of a system. During system development and deployment, it may be aggregated using standardized models along with input from observable data as the system accumulates test and operations time. Demonstrations may also be performed to determine system compliance with RMA requirements. However, these activities require thorough planning of time, resources, and approach objectives to adequately capture system RMA characteristics with acceptable confidence and risk from the customer and vendor perspectives. For these reasons, one must structure and perform a rigorous RMA Engineering effort to establish detailed RMA requirements that may be monitored and verified during system development and deployment. For more quantitative details for calculating availability, see subsection 4.8.2.6 (RMA Tools).

#### **4.8.2.3 RMA Inputs**

Inputs to the RMA Engineering process include FAA Policy, standards, NAS Enterprise Architecture, SEMP, RVCD, Concepts, OSED, Interface Control documents, requirements, descriptions of alternatives, and functional and physical architectures, as well as specific measurements and other data that may be used to analyze system performance in the interrelated RMA areas (see Table 4.8-3). The inputs used within the RMA Engineering process shall be sufficient to enable computation of the required RMA characteristics (e.g., MTBF and MTTR) and comprehensive enough to conduct the appropriate analysis.

#### 4.8.2.4 RMA Process Tasks

RMA Engineering follows the process tasks outlined in “General Specialty Engineering Process Tasks” (subsection 4.8.0.3 above). The application of an RMA program generally follows the tasks described below.

##### 4.8.2.4.1 Task 1: Obtain an Operational Services and Environmental Description

Subsection 4.8.0.3.1 generically defines this task. Although it is useful to become familiar with the full Functional Analysis description of the target system, one should focus particularly on the failure mode and maintenance aspects, as extracted from the OSED. This information is a primary input for the RMA study efforts.

##### 4.8.2.4.2 Task 2: Bound the Problem and Define Constraints on Studies and Design

Subsection 4.8.0.3.2 describes the generic aspects of this task. Subsection 4.8.2.3 (RMA Inputs) enumerates the sources of information used in developing the study constraints. Concerns that are of specific interest for defining the scope of RMA studies include:

- Reliability requirements needed
- System complexities that might mandate need for extreme parts control or a need for unique design tolerance
- Design concepts that might result in need for application of new or immature technology
- Applicability of parts control policies
- Logistics and support policies and plans
- Design guidelines
- Special requirements, if any, for tests
- Special facilities needed to perform tests
- Applicability of warranties, guarantees, and incentives
- Potential reliability problems based on past experiences

##### 4.8.2.4.3 Task 3: Select Analytic Methods and Tools

Subsection 4.8.0.3.3 generically describes this task. Specifically, RMA-related tools to be considered include:

- **Design Reviews.** Scheduling of Design Reviews of the system should be based on system complexity, such as scheduling more frequent, intensive reviews during the higher risk phases of the lifecycle.
- **Failure Reporting Analysis Corrective Action System (FRACAS).** Tracking, analyzing, and correcting problems are key activities of an RMA program. The scope of

this activity should be based on system complexity and maturity, environmental constraints, testing regimen, definition of reportable failures, and organizational roles within the FRACAS. Further details on FRACAS appear below in subsection 4.8.2.5.1.3.1.

- **Reliability Modeling.** The scope of this effort depends on many factors, including system complexity, modes of system operation, environmental constraints, maintenance philosophy, and rigor of analysis.
- **Reliability prediction.** The scope of this effort depends on the quality and quantity of historical data that is available for the system and its components; granularity of analysis (e.g., subsystem or component level); and use of results (e.g., logistics modeling, and design tradeoffs).
- **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. Details of this tasking appear below in subsection 4.8.2.5.2.1.
- **Sneak Circuit Analysis.** This task identifies latent paths that could cause undesirable behavior or inhibit desired behaviors. The task becomes more significant for analyzing critical system components and tightly coupled interfaces, or when there are frequent design changes. This effort may benefit from integration with the FMECA tasking.
- **Components Tolerance Analysis.** This task is relevant where it is important to qualify the system or its components to remain within acceptable tolerances throughout its service life.
- **Parts selection/application.** Quantity and characteristics (e.g., COTS, reliability) of procured parts and their logistical deployment affect system reliability and maintainability.
- **Environmental Stress Screening (ESS).** For less mature products, this task shakes out manufacturing defects before a program fields the system.
- **Reliability Growth Program.** This is an ongoing effort to aggregate reliability statistics as the system accumulates test and operational time. The statistics are used to infer reliability improvement as the system experiences corrective actions. Further details on the Reliability Growth Program appear below in subsection 4.8.2.5.1.3.2.
- **Reliability Qualification Tests.** These tests are performed toward the end of the Solution Implementation phase to demonstrate compliance with RMA requirements before production. The task is more significant for less mature products or products that are to be operated in conditions different from those for which they were designed.
- **Field Reliability Acceptance Tests (FRAT).** These tests ensure that system reliability as demonstrated or expected at the end of the Solution Implementation phase has not been degraded in the In-Service Management phase.

#### **4.8.2.4.4 Task 4: Analyze System Parameters to Determine System Attributes**

Subsection 4.8.0.3.4 generically describes this task. Application of RMA tools and analyses in this phase (as chosen from those described in subsection 4.8.2.6) produces system characteristics that are used as a basis for RMA requirements definition.

#### **4.8.2.4.5 Task 5: Define and Document Specialty Engineering Requirements**

Subsection 4.8.0.3.5 generically describes this task. Regarding RMA, unambiguous and measurable system RMA requirements are identified and documented based on the mission need. For example, these may be formulated as either of the following:

- A requirement with specific reliability numbers at the system or component level, at a high enough level to enable cost-effective design. An example: "The item shall have a minimum MTBF of 1,000 hours under a specified set of operating conditions."
- An operationally based reliability requirement, as in: "The system shall be able to operate 120 days without a system-inhibiting failure."

In addition to defining traditional RMA requirements, the program office may stipulate warranties, guarantees, and incentives to share risk and extend commitment from the vendor regarding the deployed system. There are many options to structuring these agreements; it is recommended that this be done in consultation with the Contracts support group.

#### **4.8.2.4.6 Task 6: Coordinate Results With Stakeholders**

Subsection 4.8.0.3.6 generically describes this task. Specifically, RMA objectives are not achieved independently of other program or project goals; so it is important to interface and coordinate with other stakeholder organizations to provide the proper context for RMA objectives. For example, as mentioned above, consideration of warranties must be coordinated with the relevant Contracts group. Other issues that could involve organizational coordination include planning and scheduling, test site arrangements, design reviews, subcontractor arrangements, system inspections, and corrective action procedures. Additional provisions must be made to coordinate with system-user representatives and system engineering groups to address logistics, maintainability, safety, and testing constraints.

#### **4.8.2.4.7 Task 7: Document the RMA Analysis in a Design Analysis Report**

Subsection 4.8.0.3.7 generically describes this task, and subsection 4.8.2.5.2 describes content specific to RMA studies.

### **4.8.2.5 RMA Outputs**

Figure 4.8-1 (at the beginning of Section of 4.8) lists the various outputs that may result from performing Specialty Engineering. The following subsections detail some of these outputs as they relate to RMA Engineering.

#### 4.8.2.5.1 Planning Criteria

The application of an RMA program generally follows the steps below. These steps shall be considered in providing planning criteria input to SE Integrated Technical Planning (Section 4.2) for the RMA Engineering effort.

##### 4.8.2.5.1.1 Step 1: Identify RMA Program Objectives

This includes formulating RMA Program objectives under which the customer and vendor agree to participate in a structured RMA Engineering effort. Factors that should be considered for these objectives include:

- **Visibility** of progress and problems to the customer and vendor during the design effort
- **Controls** to ensure that adequate standards are being applied to the design, quality, and production of the system as related to RMA
- **Correction** to provide means to find and correct problems after the design effort
- **Communication** of information concerning the above factors within the vendor organization and to the customer
- **Demonstration** to show system compliance with RMA requirements

These requirements shall be allocated to the appropriate phases of the AMS cycle of the program. Appropriate FAA-approved reliability program standards (e.g., MIL-STDs and MIL-HDBKs) shall be followed in establishing objectives and requirements to ensure that a robust RMA Program will be instituted based on the five factors above.

##### 4.8.2.5.1.2 Step 2: Structuring the RMA Program

Tasking for the RMA Program should be based on the following considerations:

- **AMS phase.** Will there be sufficient data available in the targeted phase to get full benefit from the RMA task?
- **System design.** Is the system design new, modified, or COTS? Generally, the more mature a system is, the less effort is required for RMA evaluation.
- **System complexity.** Generally, higher complexity requires more intensive RMA tasking.
- **Task utility.** Will the information provided by the task serve a constructive purpose? If the results will not be usable to correct system deficiencies, the task may not be cost effective to perform.
- **Cost.** Is the investment in the task worth the result?
- **Schedule impact.** Will the task affect the progress of the program or project?

- **Subcontractor control.** If subcontractors are involved, tasking must be considered to ensure that the prime vendor is qualifying subcontractor products for compliance with program requirements.

#### 4.8.2.5.1.3 Step 3: Establish Performance-Monitoring Processes

Plans shall be developed early in the program to define processes to monitor RMA performance throughout the system lifecycle. It is recommended that an RMA data system be incorporated early in the system's lifecycle to support such monitoring and assessment of RMA performance, and to ensure that all recorded RMA data are appropriately disseminated, analyzed, and evaluated. Two relevant methodologies—FRACAS and the Reliability Growth Program—should be planned for most RMA programs and are described below.

##### 4.8.2.5.1.3.1 FRACAS

In conjunction with an effective RMA data system, it is recommended that a closed-loop FRACAS be established to support problem detection, assessment, and correction. Such a system enables implementation and documentation of design improvements and corrections during the system development process. It also provides a tool for monitoring progress toward meeting system RMA requirements. The data collected supports tracking root causes of problems, which facilitates overcoming hurdles that may be hindering achievement of specific RMA requirements.

It is recommended that the FRACAS continue to be used during in-service operations to support upgrading of system RMA performance, in conjunction with a Reliability Growth Program (see next subsection), if necessary. Operational environments provide greater fidelity for demonstrating the actual capability of the system to meet RMA requirements.

##### 4.8.2.5.1.3.2 Reliability Growth Program

Reliability growth, sometimes called Test Analyze And Fix (TAAF), is an ongoing process of testing to identify design, material, and specification deficiencies, as well as for performing corrective engineering changes. Failures that randomly occur due to normal wear and tear which are typically corrected by replacing parts are not within the scope of this effort. Statistical methods are used to predict the system MTBF at any point in time and to estimate the additional test time required to achieve a given MTBF goal.

To ensure a successful Reliability Growth Program, the contractor shall be aggressive in promptly correcting defects. One incentive for the contractor is the tradeoff between the Reliability Growth effort and the risk of passing Reliability Qualification tests for system acceptance. This is because it is better to discover defects during the TAAF effort, where they get corrected and credited for enhancing reliability growth, than to expose them during qualification testing, where they can hinder customer acceptance.

Another factor in implementing a Reliability Growth Program is its effect on the development schedule, taking into account the efforts involved in testing for and correcting defects. Other issues to be considered include:

- **COTS or newly developed systems.** TAAF benefits are limited for COTS items, since design changes are not within the purview of the customer.

- **State-of-the-art technology.** Systems based on cutting-edge technology would be expected to have more latent defects than more mature systems, incurring more resources.
- **System complexity.** More complex systems would be expected to have more latent defects, incurring more resources.
- **Number of target systems to be deployed.** More benefit from Reliability Growth efforts are realized as the number of fielded target systems increases. This should be taken into consideration when allocating resources to TAAF.

The success of a Reliability Growth effort depends on the following:

- Quality of test facilities
- Number of test systems allocated to the TAAF effort
- Scope and integration of the FRACAS into the Reliability Growth regimen
- Experience of the developer and availability of a priori data for similar systems

It is recommended that field personnel be involved in reliability growth testing and concur in deciding when the system is sufficiently stable to warrant deployment to the field.

#### **4.8.2.5.1.4 Step 4: Report Results**

Results of the performance-monitoring effort are reported to support assessment of the progress toward meeting requirements and meeting RMA program objectives. This includes comparing predicted and demonstrated RMA versus requirements and evaluating system RMA demand throughout the system's operational life.

#### **4.8.2.5.1.5 Step 5: Use Results for Planning, Managing, and Budgeting**

Assessing progress toward meeting requirements and meeting RMA program objectives provides feedback to adjust program planning, management, and budgeting. The results may also be used to support related analyses, such as safety and logistics, and to emphasize improvements in succeeding systems.

#### **4.8.2.5.2 Design Analysis Reports**

There are various types of RMA analyses conducted and eventually documented within a Design Analysis Report. A discussion of some of the more common RMA-related analyses follows.

##### **4.8.2.5.2.1 Failure Modes and Effects Analysis**

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.

#### **4.8.2.5.2.2 Failure Modes and Effects Criticality Analysis**

FMECA identifies potential design weaknesses through a systematic analysis approach. It considers all possible ways in which a component may fail (the modes of failure); the possible causes for each failure; the likely frequency of occurrence; the criticality of failure; the 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.

Essentially, an FMECA is generated from an FMEA by adding a criticality figure of merit. More information on performing an FMECA appears in Section 9.7 of the FAA's System Safety Handbook.

#### **4.8.2.5.2.3 Fault Tree Analysis (FTA)**

FTA is another approach to FMEA. It takes on a more general, functional view than the tabular FMEA, providing more visibility into the cause of a failure effect. Details on FTA contents and the steps involved in performing an FTA appear in Section 9.3 of the FAA's System Safety Handbook.

#### **4.8.2.5.3 Requirements**

The following subsections provide general guidelines in developing candidate RMA requirements that may arise as a result of RMA Engineering analysis efforts.

##### **4.8.2.5.3.1 RMA Requirements**

For systems that are directly replacing existing systems, it is recommended that the RMA Engineering practitioner do the following:

- Locate the system being replaced within the higher level architecture
- Identify the service thread or threads that the system supports
- Determine the criticality level of the service thread; if more than one service thread is supported, use the service thread with the highest criticality level
- Use the availability associated with the service thread with the highest criticality level as the basis for the system-level availability requirement

For systems that are not replacing existing systems, it is recommended that the RMA Engineering practitioner do the following:

- Identify the criticality of the system according to the provided requirements
- Ensure that the requirements are consistent with the higher level requirements and the associated NAS Architecture implementation plan being addressed

The primary objectives in preparing the RMA provisions for a procurement package are to:

- Provide the specifications, including a system-level specification, defining the RMA requirements for the delivered system
- Define the effort required to provide the documentation, engineering, and testing to support monitoring of the design and development effort, risk management, design validation, and reliability-growth testing activities
- Provide guidance concerning the design and data required to facilitate technical evaluation of fault-tolerant design approaches, as well as programs for risk management, software fault avoidance, and reliability growth

The system-level specification serves as the basis for defining the design characteristics and performance that are expected of the system. From the standpoint of 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.

**4.8.2.6 RMA Tools**

Tables 4.8.2-1 and 4.8.2-2 list the RMA tools.

**Table 4.8.2-1. Reliability Analysis Tools and Techniques**

<b>Activity</b>	<b>What Is Done</b>	<b>Why It Is Done</b>	<b>When It Is Called For</b>	<b>When It Is Performed</b>
Alert Reporting	Document significant problem and nonconforming item data for exchange between the FAA and Government-Industry Data Exchange Program.	Identifies potential problems.	Used throughout a program (extends beyond just RMA).	As close to problem identification as possible.
Failure Mode and Effects (and Criticality) Analysis (FMEA/FMECA)	Perform a systematic analysis of the local and system effects of specific component failure modes; under FMECA, also evaluate the mission criticality of each failure mode.	Identifies potential single failure points requiring corrective action; identifies critical items and assesses system redundancy.	Recommended for consideration for all systems.	When a system block diagram is available; update throughout system design.

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Fault Tree Analysis (FTA)	Systematically identify all possible causes leading to system failure or an undesirable event or state.	Permits systematic, top-down, penetration to significant failure mechanisms.	Apply to critical (especially safety-critical) systems.	During system design.
Failure Reporting Analysis, Corrective Action System (FRACAS)	Provide a closed-loop system for documenting hardware and software anomalies, analyzing their impact on RMA, and tracking them to their resolution.	Ensures that problems are systematically evaluated, reported, and corrected.	All programs may benefit from some type of formal, closed-loop system.	Throughout system lifecycle.
Reliability Assurance Plan	Identify the activities essential in ensuring reliable performance, including design, production, and product operation.	Ensures that design risks are balanced against program constraints and objectives through a comprehensive effort calculated to contribute to system reliability over the mission lifecycle.	For all programs with reliability performance requirements.	During program planning.

Table 4.8.2-1. Reliability Analysis Tools and Techniques? Continued

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Reliability Modeling (Prediction/ Allocation)	Perform prediction, allocation, and modeling tasks to identify inherent reliability characteristics.	Aids in evaluating the reliability of competing designs.	Most hardware programs benefit where failure rates are needed for tradeoff studies, sparing analysis, etc.	Early in design.
Redundancy Switching Analysis	Perform a rigorous failure modes, effects, and criticality analysis (FMECA) at the part level for all interfacing circuits of redundant equipment.	Verifies that the failure of one of two redundant functions does not impair the ability to transfer to the second function.	Recommended for consideration for redundant equipment.	Early in design.
Reliability Tradeoff Studies	Compare all realistic alternative reliability design approaches against cost, risk, schedule, and performance impacts.	Aids in deriving the optimal set of reliability performance requirements, architecture, baselines, or designs.	Performed at some level on all systems; predictive techniques may be used.	Investment Analysis and Solution Implementation.
Reliability Growth Test  Test, Analyze, and Fix (TAAF)	Conduct test and repair cycles to disclose deficiencies and demonstrate RMA improvement with permanent corrective action as a result of engineering changes.	Provides gradual evolution of a system to a state of higher reliability through design changes to correct design, part, or specification deficiencies.	Appropriate for all hardware and software systems.	Toward the end of design and throughout the product lifecycle.

Table 4.8-7. Reliability Analysis Tools and Techniques? Continued

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Environmental Stress Screening (ESS)	Apply mechanical, thermal, or other stresses to the target system to precipitate latent defects to failure.	Identify defects in parts, materials, and workmanship as manifested in the fabrication and production of the target system.	Complex systems, stressful deployment environment, low system maturity, high system packaging density, past experience with similar systems	Product phase.
Sneak Circuit Analysis	Methodically identify sneak conditions (unexpected paths or logic flows) in circuits.	Identifies design weaknesses that could inhibit desired functions or initiate undesired functions.	Generally used only for the most safety-critical equipment.	Early in design.
Trend Analysis	Evaluate variation in data with the ultimate objectives of forecasting future events based on examination of past results.	Provides a means of assessing the status of a program or the maturity of a system or equipment and predicting future performance.	Used to track failures, anomalies, quality processes, delivery dates, etc.	Throughout the program.

Table 4.8.2-2. Maintainability Analysis Tools

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Link Analysis	Arrange the physical layout of instrument panels, control panels, workstations, or work areas to meet specific objectives (e.g., increased accessibility).	Provides as assessment of the connection between (a) a person and a machine or part of a machine; (b) two persons; or (c) two parts of a machine.	During design for maintainability.	During Mission Analysis and Investment Analysis.
Maintainability Modeling (Prediction/ Allocation)	Perform prediction, allocation, and modeling tasks to estimate the system mean-time-to-restore requirements.	Determines the potential of a given design for meeting system maintainability performance requirements.	Whenever maintainability requirements are designated in the design specification.	Early in Solution Implementation.
Maintenance Concept	Describe what, how, and where preventive and corrective maintenance is to be performed.	Establishes the overall approach to maintenance for meeting the operational requirements and the logistics and maintenance objectives.	Performed for any system where maintenance is a consideration.	During Mission Analysis and revised throughout the lifecycle.
Maintenance Engineering Analysis	Describe the planned general scheme for maintenance and support of an item in the operational environment.	Provides the basis for design, layout, and packaging of the system and its test equipment and establishes the scope of maintenance resources required to maintain the system.	A Maintenance Plan may be substituted on smaller programs in which maintainability prediction and analysis are not required.	Begins during design and iterated through development.

Table 4.8.2-2. Maintainability Analysis Tools—Continued

Activity	What Is Done	Why It Is Done	When It Is Called For	When It Is Performed
Maintenance Plan	Detail how the support program is to be conducted to accomplish the program goals.	Identifies the desired long-term maintenance characteristics of the system and the steps for attaining them.	Appropriate for all hardware programs.	During Investment Analysis and update throughout the life of program.
Reliability Centered Maintenance (RCM)	Determine the mix of reactive, preventive, and proactive maintenance practices to provide the required reliability at the minimum cost.	Minimizes or eliminates more costly unscheduled maintenance and minimizes preventive maintenance.	Appropriate for all hardware programs; generally called for as part of the maintenance concept.	During Solution Implementation.
Testability Analysis	Assess the inherent fault detection and failure isolation characteristics of the equipment.	Improves maintainability in response to operational requirements for quicker response time and increased accuracy.	Applicable to all hardware systems; however, especially appropriate where maintenance resources are available but restrained.	Early in design.
Tradeoff Studies	Compare realistic alternative maintainability design approaches against cost, schedule, risk, and performance impacts.	Determines the preferred support system or maintenance approach in accordance with risk, performance, and readiness objectives.	Performed where alternate support approaches or maintenance concepts involve high-risk variables.	Complete early in the acquisition cycle (see Section 4.6).

#### 4.8.2.7 RMA Metrics

At a minimum, RMA metrics are based on the system's MTBF (i.e., reliability), MTTR (i.e., maintainability), and availability. (See subsection 4.8.2.1.1 for further details.)

**4.8.2.8 References**

1. Guide to the Assessment of Reliability of Systems Containing Software. Document No. 89/97714. British Standards Institution, 12 September 1989.
2. *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. Aerospace Recommended Practice, ARP4761. Society of Automotive Engineers, Inc. Issued 1996-12.
3. *Reliability Engineer's Toolkit*. Rome Laboratory. Griffiss Air Force Base, April 1993.
4. *System Safety Handbook*. Federal Aviation Administration, 30 September 2000.

### 4.8.3 Human Factors Engineering

#### 4.8.3.1 What Is Human Factors Engineering?

Human Factors Engineering (HFE) is a multifaceted discipline that generates information about human requirements and capabilities and applies it to the design and acquisition of complex systems (see Figure 4.8.3-1). 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 economical decisions on personnel resources, skills, training, and costs. Embedding and integrating HFE activities into the acquisition of systems and equipment lower lifecycle costs, improve overall 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.

**Human Factors Engineering is a multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to:**

- Equipment, Systems, Software, Facilities
- Procedures, Jobs, Organizational Design, Environments
- Training, Staffing, Personnel management

**To produce safe, comfortable, and effective human performance.**

Figure 4.8.3-1. Definition of Human Factors Engineering

#### 4.8.3.2 Why Perform HFE?

Experience has proven that when people think of acquiring a system, they tend to focus on the hardware and the software. Individuals often fail to visualize the people who operate and maintain the hardware/software. The individuals and teams who operate or maintain the system have different aptitudes, abilities, and training, 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 in the National Airspace 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) and the *environment* in which the acquisition is used.

Applied early in the lifecycle acquisition management process, HFE enhances the probability of increased 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 operations costs. These benefits apply to commercial-off-the-shelf (COTS) and non-developmental items (NDI) as well as to developmental programs.

**4.8.3.3 Inputs to the HFE Process**

The FAA Human Factors Job Aid guidelines are in the FAA Acquisition System Toolset (FAST). These guidelines contain extensive information regarding integration of HFE activities into the acquisition management process. It is recommended that product teams be familiar with this information and embed HFE principles into their acquisition programs. The Human Performance Interfaces in Systems Acquisition (Table 4.8.3-1) identify and define the many classes of human interfaces that the product team may need to consider as it plans and implements equipment/system acquisition programs. Analysis of these interfaces may provide 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 4.8.3-1. Human Performance Interfaces in Systems Acquisition**

Human Interface Class	Performance Dimension	Performance Objective
<b>Functional Role Interfaces:</b> 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
<b>Information Interfaces:</b> 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
<b>Environmental Interfaces:</b> 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
<b>Operational Interfaces:</b> Procedures, job aids, embedded or organic training, and online help	Sustained performance	Ability to maintain performance over time

Table 4.8.3-1. Human Performance Interfaces in Systems Acquisition—Continued

Human Interface Class	Performance Dimension	Performance Objective
<b>Organizational Interfaces:</b> 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
<b>Cooperation Interfaces:</b> Communications, inter-personal relations, and team performance	Team performance	Ability to collectively achieve mission objectives
<b>Cognitive Interfaces:</b> Cognitive aspects of human-computer interfaces (HCI), situational awareness, decisionmaking, information integration, and short-term memory	Cognitive performance	Ability to perform cognitive operations (e.g., solve problems, make decisions, integrate information, and have situational awareness)
<b>Physical Interfaces:</b> Physical aspects of the system with which the human interacts (e.g., HCI, controls and displays, workstations, and facilities)	Operations and maintenance performance	Ability to perform operations and maintenance at workstations and worksites, and in facilities using controls, displays, equipment, tools, and other instruments.

Addressing the human performance limitations and capabilities would seem to be a daunting task unless the task was divided into its many components and unless human factors is described in some descriptive taxonomy of issues. Thus, the potential human factors risks may be reflected as elements of the human factors areas of interest listed in Table 4.8.3-2.

Table 4.8.3-2. Human Factors Areas of Interest

Human Factors Areas of Interest
1. <b>Allocation of Functional Roles:</b> 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. <b>Anthropometrics and Biomechanics:</b> Accommodating the physical attributes of its user population (e.g., from the 1st through 99th percentile levels).
3. <b>CHI (Computer-Human Interaction):</b> Employing effective and consistent user dialogues, interfaces, and procedures across system functions.

Table 4.8.3-2. Human Factors Areas of Interest—Continued

Human Factors Areas of Interest	
4.	<b>Communications and Teamwork:</b> Applying system design considerations to enhance required user communications and teamwork
5.	<b>Culture:</b> Addressing the organizational and sociological environment into which any change, including new technologies and procedures, will be introduced.
6.	<b>Displays and Controls:</b> Designing and arranging displays and controls to be consistent with the operator's and maintainer's tasks and actions.
7.	<b>Documentation:</b> 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.
8.	<b>Environment:</b> Accommodating environmental factors (including extremes) to which the system will be subjected and understanding the associated effects on human-system performance.
9.	<b>Functional Design:</b> Applying human-centered design for usability and compatibility with operational and maintenance concepts.
10.	<b>Human Error:</b> 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.	<b>Information Presentation:</b> Enhancing operator and maintainer performance by using effective and consistent labels, symbols, colors, terms, acronyms, abbreviations, formats, and data fields.
12.	<b>Information Requirements:</b> 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.	<b>I/O Devices:</b> Selecting input and output (I/O) methods and devices that allow operators or maintainers to perform tasks, especially critical tasks, quickly and accurately.
14.	<b>KSAs:</b> Measuring the knowledge, skills, and abilities (KSAs) required to perform job-related tasks, and determining appropriate selection requirements for users.
15.	<b>Operational Suitability:</b> 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.	<b>Procedures:</b> Designing operation and maintenance procedures for simplicity, consistency, and ease of use.
17.	<b>Safety and Health:</b> Preventing/reducing operator and maintainer exposure to safety and health hazards.
18.	<b>Situational Awareness:</b> Enabling operators or maintainers to perceive and understand elements of the current situation, and project them to future operational situations.
19.	<b>Special Skills and Tools:</b> Minimizing the need for special or unique operator or maintainer skills, abilities, tools, or characteristics.
20.	<b>Staffing:</b> Accommodating constraints and efficiencies for staffing levels and organizational structures.

**Table 4.8.3-2. Human Factors Areas of Interest—Continued**

Human Factors Areas of Interest	
21. <b>Training:</b>	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. <b>Visual/Auditory Alerts:</b>	Designing visual and auditory alerts (including error messages) to invoke the necessary operator and maintainer response.
23. <b>Workload:</b>	Assessing the net demands or impacts upon the physical, cognitive, and decisionmaking resources of an operator or maintainer using objective and subjective performance measures.
24. <b>Work Space:</b>	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.

#### 4.8.3.4 HFE 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. While the process flow is described in the 14 activities listed in Table 4.8.3-3, other subordinate activities (e.g., critical task analysis, target audience analysis, cognitive analysis, human-in-the-loop simulation, and HCI prototyping) are also required. A description of these subordinate tasks is in the FAA Human Factors Job Aid or in more detailed HFE reference manuals.

**Table 4.8.3-3. HFE Process Activities**

HFE Process Activities	
1.	Incorporate Human Factors Opportunities and Constraints Into the Mission Analysis and Service Level Mission Need
2.	Incorporate Human Factors Requirements in Program Requirements
3.	Incorporate Human Factors Assessment in the Investment and Business Case Analysis
4.	Incorporate Human Factors Parameters in Program Baselines
5.	Designate Human Factors Coordinator for the Service Organization(s)
6.	Establish Human Factors Working Group
7.	Incorporate Human Factors Strategy and Tasks into the Program Implementation Strategy and Planning
8.	Develop Integrated Human Factors Plan
9.	Incorporate Human Factors Requirements into System Specifications and Statements of Work
10.	Include Human Factors in Source Evaluation Criteria
11.	Conduct HFE Analyses
12.	Apply HFE to System Design
13.	Test System Against Human Performance Requirements
14.	Incorporate Human Factors Considerations in Post-Implementation Review

**4.8.3.5 HFE Process Tasks**

The following process flow provides an outline and overview of key activities in the HFE process.

<b>Activity 1: Incorporate Human Factors Opportunities and Constraints Into the Mission Analysis (MA) and Service Level Mission Need (SLMN)</b>		
<b>Product</b>	<b>Approval Authority</b>	<b>Tools and Aids</b>
Human factors input on opportunities and constraints to the SLMN	Mission analysis manager SLMN sponsor	Human Factors Acquisition Job Aid (Chapter 4) guidance on developing human factors input to the MA and SLMN  "Human Factors Integration Guide for Mission and Service Area Analysis"

**Description:**

Using the results from the MA, HFE inputs to the SLMN identify the human performance constraints and issues that need to be addressed or resolved. This information may come from operations and maintenance analyses or concepts and other documents that may provide insights into the effects of HFE constraints and limitations on mission and system performance. Since most acquisitions are evolutionary, important HFE information may be obtained from predecessor architectures, systems, or their component subsystems. Analyses and tradeoff studies may be required to determine the effects of constraints and issues on system performance. It is recommended that the existing literature and lessons learned databases be reviewed.

<b>Activity 2: Incorporate Human Factors Requirements in Program Requirements</b>		
<b>Product</b>	<b>Approval Authority</b>	<b>Tools and Aids</b>
Human factors requirements in the preliminary and final program requirements documents	Requirements development lead	Human Factors Acquisition Job Aid (Chapter 4) guidance on developing human factors requirements for requirements documents  "Guidelines for Human Factors Requirements Development"

**Description:**

The preliminary and final program requirements documents contain performance and supportability requirements that do not prescribe a specific solution. The requirements document defines the essential performance capabilities and characteristics, including those of the human component. HFE inputs to the requirements document identify human performance factors that impact system design. Cognitive, physical, and sensory

requirements are established for the operator, maintainer, and support personnel that contribute to or constrain total system performance. It is recommended that any safety, health hazards, or critical errors that reduce job performance or system effectiveness be defined, and that staffing and training concepts—including requirements for training devices, embedded training, and training logistics—also be described.

<b>Activity 3: Incorporate Human Factors Assessment in the Investment and Business Case Analysis</b>		
<b>Product</b>	<b>Approval Authority</b>	<b>Tools and Aids</b>
Human factors input to the investment and business case analysis plan	Investment and business case analysis lead	Human Factors Acquisition Job Aid (Chapter 5) guidance on developing Human Factors Assessments for the investment and business case analysis
Human Factors Assessment (including risk, cost, and benefits)		“Human Factors Assessments in Investment Analysis: Definition and Process Summary for Cost, Risk, and Benefit”

**Description:**

For each alternative being evaluated, HFE inputs to the investment and business case analysis address 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 is recommended that the analysis provide information on what is known and unknown about human performance risks in meeting minimum system performance requirements. HFE areas of interest relevant to the investment and business case analysis include:

- Human performance (e.g., human capabilities and limitations, workload, function allocation, hardware and software design, decision aids, environmental constraints, team versus individual performance)
- Training (e.g., length of training, training effectiveness, retraining, training devices and facilities, embedded training)
- Staffing (e.g., staffing levels, team composition, organizational structure)
- Personnel selection (e.g., aptitudes, minimum skill levels, special skills, experience levels)
- Safety and health hazards (e.g., hazardous materials or conditions, system or equipment safety design, operational or procedural constraints, biomedical influences, protective equipment, required warnings and alarms)

Activity 4: Incorporate Human Factors Parameters in Program Baselines		
Product	Approval Authority	Tools and Aids
Human factors performance parameters in the program baselines	Business case analysis lead	Human Factors Acquisition Job Aid (Chapter 4) guidance on developing human factors parameters for acquisition program baselines (Exhibit 300 Attachment 1) and the business case analysis (Exhibit 300 Attachment 2)  "Guidelines for Human Factors Requirements Development"

**Description:**

The program baselines established at the Investment Decision 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 Program Requirements and final Program Requirements). They reflect a progressive refinement that provides increased definition, greater granularity, and more specificity of relevant human-system performance characteristics. It is recommended that constraints, limitations, and unique or specialized training requirements, staffing levels, or personnel skill requirements be identified.

It is also recommended that, to the degree possible, the required level of human performance be based on practical measures of operational effectiveness and suitability and be stated in quantifiable terms (e.g., time to complete a given task, level of accuracy required, and number of tracks to be processed per unit time).

Activity 5: Designate Human Factors Coordinator for the Service Organization(s)		
Product	Approval Authority	Tools and Aids
Human Factors Coordinator	System engineer	Human Factors Acquisition Job Aid (Chapter 3) guidance on developing a human factors program

**Description:**

The Service Organization designates a Human Factors Coordinator to develop, direct, and monitor HFE activities during system acquisition. It is recommended that this designation 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:

- Defines human impacts and constraints during investment analysis and determines of requirements
- Evaluates human-system interfaces during market surveys, tradeoff analyses, and prototypes
- Prepares and updates HFE portions of program planning documents, procurement packages, performance criteria and measures, and data collection efforts
- Develops and analyzes operational scenarios and human-system modeling for operators and maintainers
- Reviews and assesses HFE concepts and designs
- Coordinates HFE efforts and workgroup activities
- Coordinates HFE with other disciplines

<b>Activity 6: Establish Human Factors Working Group</b>		
<b>Product</b>	<b>Approval Authority</b>	<b>Tools and Aids</b>
Human Factors Working Group Charter	System engineer	Human Factors Acquisition Job Aid (Chapter 3) guidance on human factors working groups

**Description:**

The Human Factors Coordinator may establish and chair a Human Factors Working Group (HFWG) 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 Service Organization members, with outside members participating as needed.

<b>Activity 7: Incorporate Human Factors Strategy and Tasks Into the Program Implementation Strategy and Planning</b>		
<b>Product</b>	<b>Approval Authority</b>	<b>Tools and Aids</b>
Human factors strategy and tasks in the program Implementation Strategy and Planning document	System Engineer	Human Factors Acquisition Job Aid (Chapter 3) guidance for developing human factors strategy and tasks for the acquisition program

**Description:**

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 resources
- Timing and scope of HFE activities
- 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 NDIs, COTS 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, 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.

<b>Activity 8: Develop Integrated Human Factors Planning Information</b>		
<b>Product</b>	<b>Approval Authority</b>	<b>Tools and Aids</b>
Integrated Human Factors Plan	Service Organization lead	Human Factors Acquisition Job Aid (Chapter 3) template for Integrated Human Factors Plan

**Description:**

For well-managed system acquisition programs, the Service Organization prepares an Integrated Human Factors input to the System Engineering Management Plan. (See Table 4.8.3-4 for an outline of the content.) 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
- Defining HFE implementation tasks and activities

Activity 9: Incorporate Human Factors Requirements Into System Specifications and Statements of Work		
Product	Approval Authority	Tools and Aids
Human factors requirements in the System Specification  Human Factors tasks in the Statement of Work  Human Factors data items in the Contractor Deliverable Requirements List (CDRL)  Human Factors data item descriptions	Service Organization lead	Human Factors Acquisition Job Aid (Chapter 6) guidance on formulating human factors requirements in the System Specification  Human Factors Acquisition Job Aid (Chapter 7) guidance on defining human factors tasks in the Statement of Work  Data Item Descriptions (FAA-HF-001 through FAA-HF-005) for human factors

**Description:**

The System Specification and Statement of Work translate human performance requirements and appropriate HFE work tasks to the contractor in a clear, unambiguous, and contractually binding document. The System Specification addresses the following elements to ensure that required human performance effectively influences system design:

- Staffing constraints
- Required operator and maintainer skills
- Training time and cost for formal, informal, and on-the-job skill development
- Acceptable levels of human and system performance when operated and maintained by the training population

The Statement of Work shall contain all human factors tasking to be imposed on the contractor, as well as define data deliverables in the CDRL and associated Data Item Descriptions (DID).

Activity 10: Include Human Factors in Source Evaluation Criteria		
Product	Approval Authority	Tools and Aids
Human factors source evaluation criteria	Service Organization lead	Human Factors Acquisition Job Aid (Chapter 8) guidance for specifying human factors in source selection

**Description:**

It is recommended that human performance be a candidate as a major evaluation factor in source selection. 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.

Activity 11: Conduct HFE Analyses		
Product	Approval Authority	Tools and Aids
Appropriate government or contract analyses and data such as those specified in the CDRL and DIDs	Appropriate government or contract official as designated in the CDRL (or other designated documentation)	Human Factors Acquisition Job Aid (Chapter 9) guidance for integrating human factors in system engineering Human Factors Design Standard, HF-STD-001 Human Factors Data Item Descriptions FAA-HF-001 through FAA-HF-005

**Description:**

The responsible Service Organization oversees, monitors, and reviews HFE analyses conducted by the implementation organization. These analyses may involve:

- Defining and allocating system requirements (e.g., human factors requirements analysis, staffing analysis, training analysis)
- Analyzing information flow and processing (e.g., information requirement analysis, CHI design analysis)
- Estimating operator and maintainer capabilities (e.g., task performance analysis, training performance analysis, time and motion study, safety analysis)
- Defining and analyzing physical and cognitive tasks and workloads (e.g., task analysis, job design analysis, organizational design analysis)
- Identifying and measuring human error risks and defining their mitigation and impact on design, equipment, procedures, and task performance (e.g., human reliability analysis for Reliability, Maintainability, and Availability Engineering; human factors safety analysis; and human factors risk assessment)

Activity 12: Apply HFE to System Design		
Product	Approval Authority	Tools and Aids
Implementation of Human Engineering Program Plan  Integration of Human factors requirements into system design	System engineer	Human Factors Acquisition Job Aid (Chapter 9) guidance for integrating human factors in system engineering  Human Factors Design Standard, HF-STD-001

**Description:**

HFE is applied to system design activities to optimize human-system interfaces and 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 manuals. The following are used effectively in defining human-product interfaces during system design:

- Prototypes and computer models
- Three-dimensional mockups
- Scale models
- Dynamic simulation

Activity 13: Test System Against Human Performance Requirements		
Product	Approval Authority	Tools and Aids
Test results on human performance requirements	System engineer  System test official	Human Factors Acquisition Job Aid (Chapter 10) guidance on HFE activities during test and evaluation

**Description:**

Testing to see if the system complies with human performance requirements is performed as early as possible in system development. HFE findings from design reviews, prototype reviews, mockup inspections, demonstrations, and other early engineering tests are used in planning and conducting later tests. HFE testing focuses on verifying that user personnel in the intended operational environment are able to operate, maintain, support, and control the system.

Activity 14: Incorporate Human Factors Considerations in Post-Implementation Review		
Product	Approval Authority	Tools and Aids
Assessment of the acceptability of the human-system interface and performance  Post-Deployment Human Factors Assessment Plan	System engineer	Human Factors Guidance on Conducting Human Factors Post-Implementation Reviews  FAA policy and guidance on Post-Implementation Reviews  In-Service Management Review Checklist (Section 6)

**Description**

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.

**4.8.3.6 HFE Process Outputs/Products**

Efforts to manage the HFE program, establish requirements, conduct system integration, and test and evaluate HFE compliance may result in many major and minor 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 (e.g., 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 Job Aid (and other HFE manuals), but are reflected in the following five key components of program planning and implementation.

**4.8.3.6.1 HFE Planning Criteria**

HFE planning involves developing concepts, tasks, completion dates, 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 Planning (Section 4.2).

**4.8.3.6.2 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 to specific tasks, analyzing tasks to determine human performance parameters, quantifying task parameters to permit evaluation of human-system interfaces in relation to total system operation, and identifying high-risk HFE areas.

#### 4.8.3.6.3 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 interfaces that operate within human performance capabilities, meets system functional requirements, and accomplishes mission objectives. (See Trade Studies (Section 4.6).)

#### 4.8.3.6.4 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 and resource constraints. (See Validation and Verification (Section 4.12).)

#### 4.8.3.6.5 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, and training functions.

#### 4.8.3.7 References

1. Boff, K., and Lincoln J., eds. *Engineering Data Compendium: Human Perception and Performance. Vols. 1- 3.* Wright-Patterson Air Force Base, OH: Harry G. Armstrong Aerospace Medical Research Laboratory, 1988.
2. Booher, H. R., ed. *Handbook of Human Systems Integration*, New York, NY: John Wiley & Sons, 2003.
3. Booher, H. R., ed. *MANPRINT: An Approach to Systems Integration*, New York, NY: Van Nostrand Reinhold, 1990.
4. Cardosi, K. M., and Murphy, E. D., eds. *Human Factors in the Design and Evaluation of ATC Systems.* Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, April 1995.
5. *Definitions of Human Factors Terms.* MIL-HDBK-1908, August 1999.
6. *FAA Human Factors Design Standard.* Document HF-STD-001. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, June 2003. (<http://hf.tc.faa.gov/hfds/>)
7. *Human Engineering Design Guidelines.* MIL-HDBK-759C, July 1995.
8. *Human Engineering Program Process and Procedures.* MIL-HDBK-46855A, May 1999.
9. *Human Factors Job Aid Guidelines.* Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, December 2003. (<http://fast.faa.gov/archive/v0200/human/htm/ccontent.htm>)
10. *Human Factors Policy.* FAA Order 9550.8. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, July 2005.
11. Meister, D. *Behavioral Analysis and Measurement Methods.* New York, NY: John Wiley & Sons, 1985.
12. National Research Council. *Flight to the Future: Human Factors in Air Traffic Control.* Washington, DC: National Academy Press, 1997.

13. National Research Council. *The Future of Air Traffic Control: Human Operators and Automation*. Washington, DC: National Academy Press, 1997.
14. Salvendy, G., ed. *Handbook of Human Factors and Ergonomics*. 2nd edition. New York, NY: Wiley-Interscience, 1997.
15. Sanders, M. S., and McCormick, E. J. *Human Factors in Engineering and Design*. 7th edition. New York, NY: McGraw-Hill, 1993.
16. *The National Plan for Civil Aviation Human Factors*. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, 1995.
17. Wickens, C. D. *Engineering Psychology and Human Performance*. 2nd edition, New York, NY: Harper Collins, 1992.
18. Wiener, E. L., and Nagel, D. C., eds. *Human Factors in Aviation*. New York: Academic Press, 1998.

## 4.8.4 Electromagnetic Environmental Effects and Spectrum Management

Electromagnetic Environmental Effects (E<sup>3</sup>) and Spectrum Management are two closely related areas of Specialty Engineering. They differ, however, in several ways, and the following sections discuss each area separately, starting with E<sup>3</sup>.

### 4.8.4.1 Electromagnetic Environmental Effects

E<sup>3</sup> Engineering is 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. E<sup>3</sup> activities seek to minimize a system's limitations that are due to electromagnetic factors, as well as document limitations and vulnerabilities that remain after a system's deployment.

#### 4.8.4.1.1 What Is Electromagnetic Environmental Effects Engineering?

E<sup>3</sup> 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<sup>3</sup> and gives special attention to what it calls "digital devices." The FCC defines a digital device as:

*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 . . .*

In other words, digital devices are any electronic devices using high-speed switching waveforms. These devices usually generate significant electromagnetic interference (EMI) and shall be designed to conform to government regulations on electromagnetic emissions.

All systems deployed in the NAS shall conform to government regulations. E<sup>3</sup> analyses shall be performed to ensure that all electronic systems function properly within an operational environment and that they are compatible with nonelectronic elements of that environment. These analyses shall also identify problems that could arise from changes in the environment.

There are many types of E<sup>3</sup> 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 E<sup>3</sup>. (Note: E<sup>3</sup>-related definitions appear in American National Standards Institute (ANSI) C63.14.)

##### 4.8.4.1.1.1 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<sup>3</sup>. This involves describing all EMI within the environment and vulnerabilities to systems and other elements of the environment.

It is important to develop a complete description of the normal EME within which the system, subsystem, or equipment may be required to perform. In some instances, commercial-off-the-shelf (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.

#### 4.8.4.1.1.2 Electromagnetic Compatibility

A key area of E<sup>3</sup> is Electromagnetic Compatibility (EMC). This 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. This data is then used 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. Invoking 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.

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 intentional antennas. Switching waveforms in circuits generate a wide band of EM emissions.

#### 4.8.4.1.1.3 Electromagnetic Susceptibility

EM Susceptibility (EMS) specifically deals with a system's weaknesses or lack of resiliency regarding certain EM conditions. A *susceptibility* is a condition that causes a system to be degraded. For example, conducted susceptibility refers to a system's inability to withstand an infusion of noise into its power lines. Devices that run on standard AC power shall not be susceptible to sudden brief spikes or losses of power if the power system is affected by lightning or other surges.

A system may be exposed to different operational EMEs during its lifetime. A system that degrades within certain potential EMEs is said to be *vulnerable*. A vulnerability analysis shall be conducted to determine the operational impacts of laboratory-observed susceptibilities.

#### 4.8.4.1.1.4 Hazards of Electromagnetic Radiation

Hazards of EM Radiation (RADHAZ) are areas of E<sup>3</sup> 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 sparks are formed in the air gap between two conductors.) It is difficult to locate all potential antennas and spark gaps within an EME, so it is necessary to keep the power densities of EM fields within safety margins when fuels are present.

HERP deals with the dangers of 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. Considering RADHAZ in the E<sup>3</sup> analysis ensures safety for the nonelectronic elements of an EME.

#### 4.8.4.1.1.5 Electromagnetic Pulse

An EM Pulse (EMP) is an intense burst of EMI 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.

#### 4.8.4.1.1.6 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.

#### 4.8.4.1.1.7 Lightning

Lightning gets special attention within E<sup>3</sup> 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.

#### 4.8.4.1.1.8 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.

#### 4.8.4.1.2 Why Perform E<sup>3</sup> Activities?

The following subsections discuss the key reasons for incorporating E<sup>3</sup> activities into the SE process.

##### 4.8.4.1.2.1 Government Regulations

The FCC develops and enforces government regulations relating to E<sup>3</sup>. Before a new electronic device may be sold in the United States, it shall meet the FCC's standards. These standards are in Rules and Regulations of Title 47 (Part 15) of the Code of Federal Regulations.

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 are less stringent for Class A than for Class B (household) devices. Government regulations change frequently, so it is important to obtain the most current requirements. Information is available

from the FCC Web site ([www.fcc.gov](http://www.fcc.gov)). The FCC may request a sample device of a new system to test.

#### **4.8.4.1.2.2 System Performance and Cost of Redesign**

While manufacturers and developers strive to meet government regulations, they may impose additional E<sup>3</sup> requirements on a new system to enhance product performance and customer satisfaction. Government E<sup>3</sup> 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<sup>3</sup> 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.

#### **4.8.4.1.2.3 Hazard Prevention**

Hazards of EM radiation on fuels and personnel (HERF, HERP) are important considerations. These issues may be included as part of Safety Risk Management activities.

#### **4.8.4.1.2.4 International Considerations**

EMI is increasing throughout the world. Systems that may be used outside of the United States, such as avionics, shall 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.

#### **4.8.4.1.3 Analyses of Electromagnetic Environmental Effects**

While Section 4.8.0.3 describes the Specialty Engineering process in general terms, this section specifically discusses the various E<sup>3</sup>-related analyses. Not all E<sup>3</sup> analyses discussed, however, are necessary for a given system. It is recommended that it be determined during planning which analyses are worth the time and resources.

It is recommended that E<sup>3</sup> 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<sup>3</sup> analyses increases with each subsequent phase of the SE lifecycle. Measurement procedures for evaluating a product's emissions during low-level technical analyses shall be clearly spelled out. It shall be understood how the results are to be interpreted. The EME may undergo appreciable changes at any point during a system's lifecycle. Thus, E<sup>3</sup> analyses shall be reconducted to ensure continued EMC of *each* system within the EME.

#### 4.8.4.1.3.1 Description of the Operational Electromagnetic Environment

Before any EMC analyses are conducted, it is necessary to describe the EME within which the system in question may perform. This means 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 advisable 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 system under analysis. 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).

#### 4.8.4.1.3.2 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.

It is useful to calculate the system's *electrical dimensions* before an EMC analysis is conducted. This is done to determine whether or not simple mathematical methods (e.g., Kirkchoff'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 be employed. These are a set of differential equations that describe an electric field as three-dimensional parameters (x, y, z) and time (t).

#### 4.8.4.1.3.2.1 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.

#### 4.8.4.1.3.3 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.

#### 4.8.4.1.3.4 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
- Susceptibility to Lightning
- P-Static Susceptibility
- EMP Survivability

#### 4.8.4.1.4 Outputs and Products of Electromagnetic Environmental Effects

It is important to employ E<sup>3</sup> analyses and predictions during all phases of an electronic system's lifecycle. Figure 4.8-1 (at the beginning of Section 4.8) illustrates the fundamental Specialty Engineering process and its outputs. The following sections link the outputs of E<sup>3</sup> activities to the overall SE process. However, note that all E<sup>3</sup> analyses, like other Specialty Engineering analyses, shall be documented in a Design Analysis Report.

##### 4.8.4.1.4.1 Requirements

Most E<sup>3</sup> activities result in requirements that feed the Requirements Management process (Section 4.3). This includes the Mission Need Statement, Statement of Work, specifications, and all performance-based requirements.

##### 4.8.4.1.4.2 Concerns and Issues

It is recommended that E<sup>3</sup> 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 4.10).

##### 4.8.4.1.4.3 Verification Criteria

It is critical to provide verification criteria to ensure that stated E<sup>3</sup> performance requirements are met. It is also important to provide detailed information describing how E<sup>3</sup> testing is performed and how test results are to be interpreted. This feeds the Validation and Verification process (Section 4.12).

##### 4.8.4.1.4.4 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<sup>3</sup> issues early in a system's development.

#### 4.8.4.2 Spectrum Management

The radio frequency (RF) spectrum is that portion of the EM spectrum used for *deliberately* transmitting and receiving signals. It is a finite set of frequencies that must be divided efficiently between various government and civilian industries. The FAA, Air Force, and Navy are the top three spectrum users in the Federal Government. The FAA's numerous communication, 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 within the NAS.

#### **4.8.4.2.1 What Is Spectrum Management?**

FAA Order 6050.19 states that “the radio spectrum is a scarce and limited resource” and that “the FAA is committed to new spectrum-efficient technologies and procedures to preserve this precious resource.”

Spectrum Management includes distributing the FAA’s share of the RF spectrum among NAS systems, integrating new RF technologies into the existing NAS, monitoring RF activity to ensure that NAS RF systems do not interfere with one another, and investigating external sources of RF Interference (RFI) that may degrade performance of NAS systems.

##### **4.8.4.2.1.1 Coordination With Technical Operations Services**

The Air Traffic Organization’s (ATO) Office of Technical Operations Services (formerly Spectrum Policy and Management - ASR) oversees Spectrum Management within the FAA. All project teams developing systems that require RF usage shall coordinate with Technical Operations Services to ensure that all Spectrum Management issues are addressed correctly, including assigning RF bands. Project teams shall contact Technical Operations Services early in the development process and request guidance on spectrum issues.

Technical Operations Services 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 point 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 NAS operating in an interference-free electromagnetic environment. FMOs can also engineer local or “site-specific” radio frequencies for approval by Technical Operations Services.

#### **4.8.4.2.2 Why Perform Spectrum Management?**

Spectrum Management applies only to systems that transmit RF signals. The following sections discuss the key reasons for incorporating Spectrum Management into the SE process.

##### **4.8.4.2.2.1 Spectrum Management Is Required for All RF Systems**

The U.S. Office of Spectrum Management assigns RF bands to government agencies and civilian industries. Federal law prohibits RF usage outside the assigned bands.

The ATO’s Technical Operations Services oversees the FAA’s assigned RF bands. It is *mandatory* for project teams developing RF systems to collaborate with Technical Operations Services to obtain specific RF band assignments.

Technical Operations Services continues Spectrum Management activities throughout a system’s lifecycle (e.g., frequency reassignments, RFI investigations).

#### **4.8.4.2.2.2 RF System Performance**

Spectrum Management is necessary to maintain 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.

#### **4.8.4.2.3 Activities of Spectrum Management**

Spectrum Management activities involve identifying and maintaining an RF system's transmission frequencies.

##### **4.8.4.2.3.1 Initial RF Band Assignments**

The ATO's Technical Operations Services will assign frequency bands for operational use with new NAS systems. A new RF system cannot be introduced into the NAS without obtaining frequency assignments.

##### **4.8.4.2.3.2 RFI Detection and Reporting**

New systems must be tested to ensure that they do not transmit noise that may interfere with other RF systems. Technical Operations 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.

##### **4.8.4.2.3.3 RF Band Modifications**

At any point during a system's lifecycle, Technical Operations Services may change frequency band assignments for any or all NAS systems. Reassignments may be needed because of integration of new RF systems into the NAS, changes in NAS 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.

#### **4.8.4.2.4 Outputs and Products of Electromagnetic Environmental Effects**

Figure 4.8-1 illustrates the fundamental Specialty Engineering process and its outputs. 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.

##### **4.8.4.2.4.1 Planning Criteria and Initial Requirements Document**

During the early Mission Analysis stage, determining the need and submitting a request for spectrum support to Technical Operations Services is a priority for an RF system team. The initial requirements document process is not complete until the Spectrum Planning Subcommittee approves the request. The feedback from Technical Operations Services shall

feed the Integrated Technical Planning process (Section 4.2) and the Requirements Management process (Section 4.3).

#### **4.8.4.2.4.2 Requirements and Constraints**

Technical Operations Services may impose requirements and/or constraints on an RF system at any stage of its lifecycle. These shall be used to feed the Requirements Management process (Section 4.3).

#### **4.8.4.2.4.3 Verification Criteria**

Technical Operations Services requires validation for any RF system under development that ensures spectrum usage of the system is within the approved bounds. This feeds the Validation and Verification process (Section 4.12).

#### **4.8.4.3 References**

For FAA-related subject matter expertise in E<sup>3</sup> and Spectrum Management, contact ATO's Office of Technical Operations Services. Additional sources of information on E<sup>3</sup> and Spectrum Management include:

##### **4.8.4.3.1 Policy Guidelines**

NTIA (2004), "Manual of Regulations and Procedures for Federal Radio Frequency Management (May 2003 Edition, 2004 Revision)," U.S. Department of Commerce, National Telecommunications and Information Administration, Washington, DC.  
<http://www.ntia.doc.gov/osmhome/redbook/redbook.html>.

DOT, "Radio Frequency Spectrum Use," DOT Order 5420.3, U.S. Department of Transportation, Washington, DC.

FAA (2000), "Radio Spectrum Planning," FAA Order 6050.19E, U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 30 June.

FAA (2001), "Electronic Equipment, General Requirements," Section 3.3.2 "Electromagnetic Compatibility" FAA-G-2100G, U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 22 October.

FAA (2002), "Radio Spectrum Plan 2001-2010 (2002 Revision)," U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 30 September.  
<http://www.faa.gov/ats/aaf/asr/library/docs/RSP-2002.pdf>.

FAA (1998), "Spectrum Management Regulations and Procedures Manual," FAA Order 6050.32A, U.S. Department of Transportation, Federal Aviation Administration, Washington, DC, 01 May.

##### **4.8.4.3.2 Testing Guidelines**

RTCA (1997), "Environmental Conditions and Test Procedures for Airborne Equipment," (With Three Changes Issued), RTCA/DO-160D, RTCA, Inc., Washington, DC.

DoD, (1999), "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," MIL-STD-461E, U.S. Department of Defense, Washington, DC, 20 August.

SAE (1999), "Electromagnetic Interference Measurement Antennas; Standard Calibration Method," ARP958, SAE International, Warrendale, PA, March. <http://www.sae.org/>

IEEE (1979), "IEEE Standard Test Procedures for Antennas," IEEE Std-149-1979, Institute of Electrical and Electronics Engineers, New York, NY. (Reaffirmed in 2003), ISBN 1-5593-7609-0. <http://www.ieee.org>

IEEE (1998), "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.

#### **4.8.4.3.2 Web Sites**

[www.fcc.gov](http://www.fcc.gov)

FCC

[standards.ieee.org](http://standards.ieee.org)

ANSI/IEEE

[www.jsc.mil/jsce3/e3prg.asp](http://www.jsc.mil/jsce3/e3prg.asp)

Joint Spectrum Center, E3 Engineering Support

## 4.8.5 Quality Engineering

Quality Engineering (QE), sometimes called Quality Assurance (QA), is a Specialty Engineering discipline within System Engineering.

### 4.8.5.1 What Is Quality Engineering?

QE is an objective analysis of all planned and systematic activities to ensure that a product or service fulfills requirements and is of the highest quality. This includes analysis of any proposed acquisition, from the Mission Analysis phase of the Acquisition Management System (AMS) through the Solution Implementation phase. Such analysis ensures that program Requirements (see Requirements Management (Section 4.3)), including the Service Level Mission Need (SLMN), are allocated properly to the physical architecture of the solution system (see Synthesis (Section 4.5)). Additionally, QE analysis evaluates a system's ability to meet its requirements and to mitigate product defects before production of the system begins. Further, QE analysis identifies development and deployment metrics to ensure that the system is designed and produced to provide maximum benefit to the stakeholders.

QE is also a philosophy and set of guiding principles that are the basis for a continuously improving organization. In recent years, QE has shifted toward designing quality into the product, rather than trying to inspect quality into a poor product after it has been produced.

Thus, QE has become a means of documenting how things will be done, and it should be addressed early in the AMS cycle. Early participation in the quality process at all levels of an organization helps to determine general, high-level quality requirements within the preliminary Program Requirements (pPR).

### 4.8.5.2 Why Perform Quality Engineering?

QE is performed to:

- Monitor quality within the FAA using ANSI/ISO/ASQ Q9001-2000, WI-200-01 "ASU-200 ISO 9001 Work Instructions Quality/Reliability Officer Guidebook." This is the Software Quality Assurance (SQA) Model of the FAA Air Traffic Organization (ATO), Operations Planning (ATO-P). (ATO-P is composed of many former organizations, including ASU-200.) The model is consistent with the FAA Integrated Capability Maturity Model (FAA iCMM).
- Reduce costs and improve product performance
- Comply with FAA Order 4630.8, "Quality Assurance Policy," and AMS paragraph 3.10.4

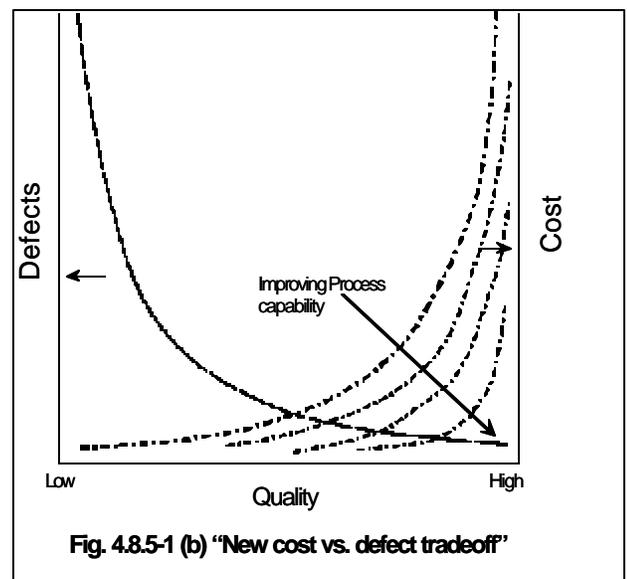
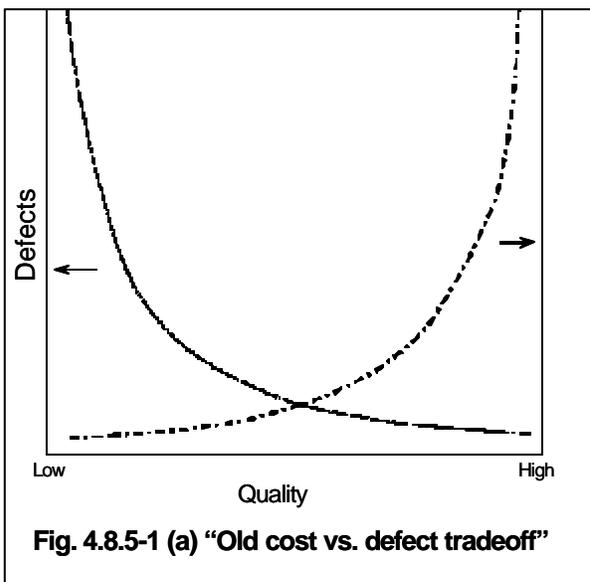
FAA Order 4630.8 requires the FAA to institute a quality program/system for National Airspace System (NAS) acquisitions of all systems, equipment, materials, and services. In the past, FAA-STDs-013, -016, and -018 quality specifications were placed on NAS programs. Currently, International Standards ANSI/ISO/ASQ Q9001-2000 are included in new NAS contracts to reflect advances in the quality sciences.

Specific requirements of AMS paragraph 3.10.4 can be easily accessed in the FAA Acquisition System Toolset (FAST) at [http://fasteditapp.faa.gov/ams/do\\_action?do\\_action=LinkSection&contentUID=4&sectionNumber=3.10.4](http://fasteditapp.faa.gov/ams/do_action?do_action=LinkSection&contentUID=4&sectionNumber=3.10.4).

The FAA iCMM, v. 2.0 (see <http://www.faa.gov/ipg/pif/icmm/index.cfm>) describes characteristics for assessing efficient internal FAA processes. Process Area 15 (PA15) addresses Quality Assurance and Management. The FAA iCMM quality focus is to ensure the quality of the product or service, ensure the quality of the processes to generate or provide the product, and provide management visibility into the processes and products. However, the iCMM, as a high-level document, provides criteria to determine if quality is being met, but it does not contain the detailed process. This section provides that process.

In addition, the practice of QE promotes reduced costs and risks in upgrading the NAS. To some, this concept is contradictory. Many believe that improved quality only results from more inspection, which increases costs in both time and money. Others believe that it takes much longer to design and manufacture a higher quality product. Figure 4.8.5-1 (a) shows a balance between costs and defects, where moving to either side of that balanced position results in higher costs.

Many industries have proven these beliefs to be wrong. They have shown that inspection alone does not improve quality. In fact, many companies produce high-quality products at lower costs. Organizational focus throughout the lifecycle is what really resolves quality issues. By improving processes (see Figure 4.8.5-1 (b)), companies decrease defects while maintaining the same or lower costs; and decreasing product defects usually improves system performance and productivity. The net result is that stakeholders are more satisfied with the products or services.



### 4.8.5.3 Quality Engineering Process Tasks

QE follows the basic process tasks outlined in “General Specialty Engineering Process Tasks” (subsection 4.8.0.3).

Additionally, for software quality assurance, there are specific process tasks in the “Software Quality Assurance and Industrial Evaluation Guidebook” (<http://www.asu.faa.gov/ASU-200/QualitySystem/WI-250-01.doc>). QE analysis supports the SLMN analysis, Investment Analysis Team, and the Service Organization. QE provides high-level quality plan recommendations during the Mission Analysis phase, but primarily participates in the Investment Analysis and Solution Implementation phases.

#### 4.8.5.3.1 Mission Analysis Phase

QE involvement is at a macro level during the Mission Analysis phase. QE participates in developing or revising the SLMN. QE supplies estimates of quality costs to the system engineer member of the Service Level Mission Need Development Team, who shares these inputs with the team. Additionally, QE reads, reviews, and comments on the SLMN as it is developed, ensuring that QE concerns are expressed and documented. QE participates in the alternatives analysis, assisting in evaluating alternatives and commenting on technological feasibility of the alternatives, especially technological maturity. QE also contributes to the concept of use definitions, which may reflect back to the technological feasibility or interfaces of the proposed alternative. All these Mission Analysis activities contribute to development of the pPR, which is the Exhibit 300 Attachment 1.

#### 4.8.5.3.2 Investment Analysis Phase

During Investment Analysis, the QE process reviews the pPR (to ensure that all QA requirements are included) and provides inputs to the Implementation Strategy and Planning (ISAP) (Exhibit 300 Attachment 3). These inputs include general descriptions of the QE philosophy, baseline quality requirements, and constraints concerning risk management. QE analysis outputs are provided to Requirements Management (Section 4.3), Integrated Technical Planning (Section 4.2), the Service Organization, and Investment Analysis Team.

##### 4.8.5.3.2.1 Develop Acquisition Strategy

QE helps develop the overall strategy for implementing the acquisition program within the cost, schedule, performance, and benefit parameters of the program’s Exhibit 300.

QE develops the QA section of the ISAP, and recommendations for the ISAP should include the following:

- Establish QA controls, including contractor status reporting, quality metrics, peer review, and independent verification and validation
- List QA standards with justification for selecting those quality standards
- Select automated tools used to manage and communicate QA actions and activities
- Ensure that the vendor’s software Quality processes are evaluated and scored as a part of the source selection

- Monitor the vendor's software Quality processes after award
- Establish Quality milestones
- Estimate Quality funding requirements by fiscal year
- Estimate appropriate Quality resources by fiscal year

Outputs and recommendations for ISAP should be provided in writing and copies of recommendations retained. Figure 4.8.5-2 is an example of a simple program support plan form.

## Program Support Plan

**SECTION A: (Example) PROGRAM INFORMATION**

<b>ANALYST:</b> (Name of Program Analyst) Jane Q Engineer		<b>DATE:</b> (Date prepared) 01/01/2010	
<b>PROGRAM NAME and DESCRIPTION:</b> (Program name (acronym) and description) Next Upgrade Backup System (NUBS)			
<b>TYPE OF PROGRAM:</b> (Commercial-off-the shelf/non-developmental item, etc.) Design/development		<b>EST. CONTRACT AWARD DATE:</b> (Anticipated award date) 06/06/2010	
<b>EST. CONTRACT END DATE:</b> (Anticipated end date) 08/08/2015		<b>EST. SOFTWARE KSLOC:</b> (Estimated thousands source lines of code) 200 KSLOC	
<b>CAS CODE:</b> (Cost Accounting Standard Code) 00010000		<b>EST. SOFTWARE CSCIs:</b> (Estimated number of Computer Software Configuration Items) 20	

**SECTION B: PRE-AWARD INPUT AND ACTIVITIES** (List pre-award input provided: i.e., document/review/evaluations/activity as applicable. Insert additional rows as necessary for each item.)

<b>INVESTMENT ANALYSIS:</b> INPUT/ACTIVITY (Example)	COMMENTS	Due Date	Date Complete
Preliminary Program Requirements, Exhibit 300 Attachment 1	Review preliminary Program Requirements and provide comments to service organization	1/2010	
<b>PROGRAM PLANNING:</b>			
INPUT/ACTIVITY (Example)	COMMENTS	Due Date	Date Complete
Implementation Strategy and Planning	Prepare Quality Assurance section of ISAP and review and comment	1/2011	
Source Selection Plan	Prepare Quality Assurance portion of Source Selection Plan	3/2011	
<b>SIR/CONTRACT:</b>			
INPUT/ACTIVITY (Example)	COMMENTS	Due Date	Date Complete
Statement of Work (SOW)	Prepare Quality Assurance Section of SOW	2/2011	
Screening Information Request (SIR)	Prepare Quality Assurance Section of SIR	4/2011	
Contract	Prepare Quality Assurance portion of SIR, Section E, Quality Assurance Critical Design Review, and Data Item Descriptions	5/2011	
<b>EVALUATION ACTIVITIES:</b>			
INPUT/ACTIVITY (Example)	COMMENTS	Due Date	Date Complete
Review Quality Assurance Plans	Review and recommend actions regarding Quality System Plans	4/2011	
Review Software Quality Assurance Plans (SQAP)	Review and recommend actions regarding SQAPs	4/2011	
Review Test Plans	Review and comment	4/2011	

**SECTION C: POST- AWARD MILESTONES/ACTIVITIES**

MILESTONE/ACTIVITY (*Example*)      COMMENTS      Date Scheduled      Date Complete

<b>POST-AWARD CONFERENCE:</b>	Estimated to be within 1 month of contract award	TBD	
<b>DESIGN REVIEWS:</b>	Preliminary Design Review, Software Design Review, Final Design Review, and Functional Configuration Audit/Physical Configuration Audit	“	
<b>TECHNICAL REVIEWS:</b>	Technical Interchange Meetings, Code walkthroughs, and Test Readiness Reviews	“	
<b>TESTS:</b>	Design Quality Test, Factory Acceptance Test, and Site Acceptance	“	
<b>DELIVERIES:</b>	Initial delivery no later than 12 months after contract award — schedule per contract	“	
<b>INSTALLATION:</b>	Initial installation 16 months after contract award	“	

**SECTION D: CONTRACT INFORMATION**

(*Example*)

<b>CONTRACT #:</b> FA01-C-10- 000000	<b>\$VALUE AT AWARD:</b> \$80,000,000
<b>CONTRACTOR:</b> Acme Corp.	<b>LOCATION:</b> Any City, OK
<b>CONTRACT AWARD DATE:</b> Estimated 6/2010	<b>TOTAL QUANTITY ORDERED:</b> 100 Systems
<b>ACCEPTANCE:</b> Preliminary: QRO Source Final: Destination	<b>TYPE OF CONTRACT:</b> Cost Plus Fixed Fee
	<b>GOVERNMENT FURNISHED PROPERTY/CONTRACTOR ACQUIRED PROPERTY:</b> Next Upgrade Backup System NUBS Test Set

**SECTION E: QRO STAFFING ESTIMATES**

(*Example*)

<b>FY: 2010</b>	<b>QTR 1</b>	<b>QTR 2</b>	<b>QTR 3</b>	<b>QTR 4</b>	<b>YR 2</b>	<b>YR 3</b>	<b>YR 4</b>	<b>YR 5</b>	<b>YR 6</b>
<b>Software</b>	0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
<b>Hardware</b>	0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
<b>TOTAL</b>	0.00	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0

Figure 4.8.5-2. Sample Product Plan

**4.8.5.3.2.2 Augment Program Work Breakdown Structure**

QE helps to develop the program Work Breakdown Structure (WBS). The WBS is a logical, tailored arrangement of work elements needed to deliver systems, and it should be tailored to the acquisition program and clearly describe the product to be developed. One must be familiar with the WBS to understand the program’s technical objectives, specification tree, and configuration items.

**4.8.5.3.2.3 Establish Program Metrics**

Program metrics, including QA metrics, aid program management by identifying problems, measuring product quality, and assessing process conformance and effectiveness. QE determines the appropriate QA program metrics used to evaluate progress, monitor critical issues and risks, and

provide information for cost and schedule estimates. Each metric should be related to and defined in terms of a specific process, risk factor, or key program element. Metrics should include descriptions; quantitative bounds; and the identity of the parties responsible for identifying, collecting, and analyzing data as well as for reporting the results of metrics analysis. Program metrics should be scaled appropriately to the overall program. As determined by QE, the metrics should include:

- A measurement action plan
- Risk management metrics
- Earned value management metrics
- Software design and development metrics

#### **4.8.5.3.2.4 Contribute to Implementation Strategy and Planning, Exhibit 300 Attachment 3**

The ISAP consists of all planned actions and activities, including QE actions and activities, to successfully complete the program. The ISAP's Quality Assurance section, at a minimum, includes Contractor Status Reporting, In-Plant Quality/Reliability Officers (QRO), Independent Validation and Verification, and Contractor Software Process Monitoring activities. QE activities need to be integrated into the system design, production, and deployment activity plans. There may be cost and schedule estimates that need to incorporate quality work efforts and tasks defined in the ISAP.

#### **4.8.5.3.3 Solution Implementation Phase**

Following the investment decision, QE participates in the acquisition strategy during the Solution Implementation Phase, which includes Contracting Support (see lower half of Table 4.8.5-1) and Post-Award Activities. The QE provides the bulk of the analysis during this time.

##### **4.8.5.3.3.1 Contracting Support**

The contracting stage of the Solution Implementation phase begins after the Final Investment Analysis Decision. Contracting covers all activities that lead to contract award, including preparing the Screening Information Request (SIR), evaluating offers, and selecting the source.

QE prepares the QA portions of the SIR, the Statement of Work (SOW), Contract Data Requirements Lists (CDRL), Data Item Descriptions (DID), Instructions to Offerors, and the contract itself. QE assists in developing the System Specification, Contract WBS, Evaluation Plan, and Selection Criteria. Additionally, QE evaluates offerors' proposals, providing recommendations to the source selection official for making the down-selection or award decision (see Table 4.8.5-1).

Table 4.8.5-1 QE Task/Products Aligned With Contract Phase

Solution Implementation Phase	
Pre-Contract Award	QE Tasks or Products
Prime Contract WBS	<ul style="list-style-type: none"> <li>Review WBS</li> <li>Comment on program planning, control, communications, cost estimates, and schedules</li> </ul>
System Specification	Evaluate and comment on considerations in these areas: <ul style="list-style-type: none"> <li>Functional</li> <li>Operational</li> <li>Technical</li> </ul>
SIR	<ul style="list-style-type: none"> <li>SOW</li> <li>CDRL</li> <li>DIDs</li> </ul>
Evaluation Criteria	Identify key characteristics that enable evaluators to distinguish between proposals: <ul style="list-style-type: none"> <li>Contractor Assessment Criteria:               <ul style="list-style-type: none"> <li>Soundness of Approach</li> </ul> </li> <li>Specific Criteria:               <ul style="list-style-type: none"> <li>Technical, cost, business, and program management</li> </ul> </li> </ul>
Evaluation Plan	Contribute to development of plan as needed, tailored to specific needs of the program
Proposal Evaluation	<ul style="list-style-type: none"> <li>Track changes to QA requirements</li> <li>Review bidders' QA plans</li> <li>Monitor changes to CDRL</li> <li>Identify changes to DIDs</li> </ul>
<b>Post-Contract Award</b>	
Transition	<ul style="list-style-type: none"> <li>Transition to assigned QRO</li> <li>Facilitate communication between QRO and the service organization</li> <li>Assist QRO with QA Plan</li> <li>Attend Integrated Product Team meetings</li> </ul>

#### 4.8.5.3.3.1.1 Develop Prime Contract Work Breakdown Structure

The contract WBS identifies the program work activities to complete the program and partitions and assigns responsibility for completing the activities to contractors, in-house resources, and support contractors. The prime contract WBS covers software and hardware design and development, system test, integration, and installations and identifies the independent operational test and evaluation activities. QE reviews the WBS and comments on the program planning, control, communications, cost estimates, and schedules.

#### 4.8.5.3.3.1.2 Review System Specification

The System Specification translates requirements in the high-level initial requirements document into physical system requirements that can be partitioned and allocated to specific hardware and software

configuration items. In reviewing the System Specification, QE evaluates the functional, operational, and technical considerations of the program.

#### **4.8.5.3.3.1.3 Develop and Refine Screening Information Request**

The primary items included in the SIR are the SOW, CDRL, DIDs, instructions, conditions and notices to offerors, and evaluation criteria. QE provides input and recommendations on all of these items. QE relies on sound quality principles and past experience to tailor the Quality plan to fit program needs. Thus, the analysis should:

- Specify the appropriate Quality requirements (i.e., ISO-9000-2000 and FAA-STD-026A)
- Determine whether bidders should provide quality and SQA Plans
- Define the program-specific Contract Data Requirement for the Quality and SQA Plans
- Tailor the DIDs to convey requirements to the contractor

#### **4.8.5.3.3.1.4 Form Evaluation Criteria**

QE assists in establishing the evaluation criteria to select contractors. These criteria define the selection factors and formally communicate FAA requirements to industry. Evaluation criteria must contain clear and sufficient technical guidance so that the contractor knows how the system is to perform. Evaluation criteria are included in both the evaluation plan and solicitation and typically fall into two general types:

- Assessment criteria—to assess soundness of approach and compliance with requirements
- Specific criteria—to assess technical, cost, business, and program management capabilities

Evaluation criteria also address logistics support, quality assurance, configuration management facilities, and subcontracting. Requirements included in the evaluation criteria should have a clearly defined scope and be consistent, sufficiently detailed, and appropriate for the established program needs (see Requirements Management (Section 4.3)). The primary concern is to determine the appropriate Quality evaluation criteria for the program. The following should be considered:

- Adequacy of Quality Assurance and Software Quality Assurance Plans
- Evidence of the contractor's ability to comply with recommended quality requirements
- Evidence of the contractor's ability to comply with recommended software quality requirements
- Need for an evaluation of a contractor's manufacturing capabilities
- Need to evaluate contractor's process controls

- Need to conduct software capability estimate evaluation or some other evaluation methodology (e.g., Software Assurance, RTCA DO-178B, “Software Considerations in Airborne Systems and Equipment Certification”)

Evaluation criteria comments and recommendations should focus on key characteristics that enable evaluators to distinguish among proposals.

#### **4.8.5.3.3.1.5 Prepare Evaluation Plan**

Working with the service organization, System Engineering helps develop an evaluation plan tailored to the specific needs of the acquisition. The plan identifies the source-selection official and members of the evaluation team(s); contains the source evaluation criteria; defines evaluation methods and processes; establishes the evaluation schedule; and contains any other information related to source selection. There should be a Quality representative on the evaluation team. The completed and approved plan must be completed before the SIR is released.

#### **4.8.5.3.3.1.6 Prepare Screening Information Request for Prime Contract**

A SIR solicits documentation from offerors that the service organization uses to identify the offeror that provides the government the best value. The documentation includes qualification information, screening information, and requests for offers, as well as presentations, proposals, or binding offers. The type and number of SIRs issued depend on the acquisition and the service organization’s source-selection approach. SIR preparation activities may include:

- Reviewing and providing input to the proposed SOW
- Reviewing and commenting on the proposed System Specification
- Reviewing and commenting on the WBS
- Determining and recommending appropriate Quality Requirements (e.g., ISO 9001, etc.)
- Preparing Quality System program evaluation criteria for the SIR
- Reviewing the CDRL to determine the review and/or approval process
- Assisting the service organization in finalizing Test Requirements for the SIR
- Assisting the service organization in determining appropriate reliability requirements (see Requirements Management (Section 4.3))
- Preparing descriptions of additional screening elements (e.g., establishment and maintenance of contractor parts support depot) with the service organization

#### **4.8.5.3.3.1.7 Evaluate Proposals for Prime Contract**

QA capabilities of the bidders submitting proposals are critical to the service organization's evaluation of the proposals' validity. Proposal evaluation activities relating to Quality include:

- Evaluating any proposed changes to QA requirements
- Evaluating bidders' proposed QA plans
- Reviewing any proposed changes to CDRL items
- Reviewing any proposed changes to DIDs

#### **4.8.5.3.3.2 Post-Award Activities**

Following contract award, the contractors and subcontractors begin engineering and system integration activities to produce and field systems. The FAA oversees the contractor's work to ensure that the system being built meets functional and operational requirements and is installed, integrated, supported, and maintained throughout the system lifecycle. QE continues to support programs controlled by service organization following contract award; however, QE transfers the primary QA work to the QRO. This successful transition and continued service organization and QRO support are critical to the continuity of the Quality program in the acquisition process.

QE and the QRO must coordinate activities and establish effective working relationships within the service organization and with the contractor. To establish and maintain this relationship during System Development, QE must:

- Ensure transition of the program to the assigned QRO
- Facilitate communication between the QRO and the service organization
- Assist QRO with the QA program
- Participate in service organization weekly/biweekly meetings

#### **4.8.5.3.3.2.1 Ensure Program Transition to Quality/Reliability Officer**

QE must ensure transition of the program to the QRO to ensure smooth development of the FAA in-plant QA program. Transitioning activities include:

- Briefing the QRO on the program and Quality issues
- Ensuring that the QRO has all documents needed to help establish the FAA in-plant Quality system
- Introducing the QRO to the service organization

- Assisting in establishing a working relationship with the QRO, service organization, and the contractor
- Assisting the QRO in setting up the FAA Quality system
- Assisting the QRO in preparing and submitting recommendations to the contract officer and service organization for the contract, as well as contract requirement changes, such as further tailoring ISO requirements or changes to the Quality System Plan
- Providing tailored SQA Model Guidance for software-intensive programs

#### **4.8.5.3.3.2.2 Support QRO–Service Organization Communication**

QE attends service organization contract meetings to discuss quality-related issues and stay abreast of program developments.

**Only QROs and individuals with specific delegated authority from the Contracting Office can deal directly with the contractor.**

The group shares program information, including all reports and plans developed. The information exchange and coordination of efforts should be open, timely, and focused on supporting the service organization.

#### **4.8.5.3.3.2.3 Assist QRO With Quality Assurance Plan**

QE supports the assigned QRO, who inherited primary responsibility for the FAA Quality program, following contract award and transition of the FAA Quality program to the QRO. When requested by the QRO and service organization, QE assists in post-award activities.

#### **4.8.5.4 Quality Engineering Outputs/Products**

QE outputs consist of Design Analysis Reports, which support Mission Analysis, Investment Analysis, or Solution Implementation Phases. Additionally, the sample Program Support Plan (Figure 4.8.5-2) would be an output of the Investment Analysis Phase.

#### **4.8.5.5 References**

There are a variety of sources of information about Quality Engineering within the FAA, private industry, research institutions, and organizations and consortiums. The following subsections list books and documents and Internet sources that may further reader understanding of this process.

##### **4.8.5.5.1 Books and Documents**

1. *ASU-250 Software Quality Assurance and Industrial Evaluation Guidebook (WI-250-01)*. Washington DC: Federal Aviation Administration, 2002.
2. *International Council on Systems Engineering (INCOSE) System Engineering Handbook*. Version 2.0. Seattle, WA: INCOSE Central Office, 2002.
3. Martin, James N. *Systems Engineering Guidebook*. Boca Raton, FL: CRC Press LLC, 2000.

4. Sage, Andrew P., and Rouse, William B. *Handbook of Systems Engineering and Management*. New York, NY: John Wiley & Sons, Inc., 1999.
5. *Systems Engineering Capability EIA 731*. Electronic Industries Association, 1998, pages 79–81.
6. *The Federal Aviation Administration Integrated Capability Maturity Model® (FAA-iCMM®), Version 2.0*. Washington DC: Federal Aviation Administration, September 2001, specifically Process Area 15.

#### **4.8.5.5.2 Web Sites**

<http://fast.faa.gov/>: The Federal Aviation Administration Acquisition System Toolset; contains AMS Policy.

[www.asq.org](http://www.asq.org): The American Society for Quality, 600 North Plankinton Avenue, Milwaukee, WI 53203; or P.O. Box 3005, Milwaukee, WI 53201-3005.

[www.qualitydigest.com](http://www.qualitydigest.com): Quality Digest magazine online, Quality Digest, 40 Declaration Drive, Suite 100, Chico, CA 95973.

[www.qualitymag.com](http://www.qualitymag.com): Quality Magazine, 1050 IL Route 83, Suite 200, Bensenville, IL 60106.

[www.isixsigma.com](http://www.isixsigma.com): i Six Sigma; presents discussions and articles about process controls using Six Sigma methodologies.

## 4.8.6 Information Security Engineering

Information Security Engineering (ISE) is a specialty engineering discipline within System 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 and the Federal Information Security Management Act (FISMA) of 2002, establishes a clear legal basis for information security risk management of Federal information technology (IT) resources. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, establishes policy for managing Federal information resources and implements the law within the Executive Branch. Appendix III of Circular A-130, Security of Federal Automated Information Resources, establishes a minimum set of management controls for Federal programs. Appendix III defines Federal agency responsibilities for the security of automated information and requires that an agency official authorize operation of each IT system.

FAA Order 1370.82 has implemented OMB Appendix III by defining the Security Certification and Authorization Package (SCAP) as the basis for security authorization by the appropriate FAA official.

FAA Order 1370.82 states the FAA basic security policy:

*The FAA shall ensure that security is provided commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information for all agency information collected, processed, transmitted, stored, or disseminated in FAA information systems and in information systems used on behalf of the FAA. The FAA shall also ensure that systems and applications used by or for the FAA provide appropriate confidentiality, integrity, authenticity, and availability.*

Further, the order describes roles and responsibilities related to certification and authorization (C&A) of IT products and systems within the FAA (e.g., Designated Approving Authority (DAA), Information System Security Manager (ISSM), or Certifying Agent (CA)).

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.

### 4.8.6.1 Perform Information Security Engineering

In performing ISE, system 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 subsection 4.8.6.2, 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, produce 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 Requirements Management (Section 4.3)) 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 4.8.6-1 illustrates these drivers, which are:

- **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 commercial-off-the-shelf (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 Directive 7 (HSPD-7) 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 expands vulnerabilities to systems' confidentiality, integrity, and availability unless the FAA properly addresses security.
- **Rising Terrorists and National Threats.** The 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.

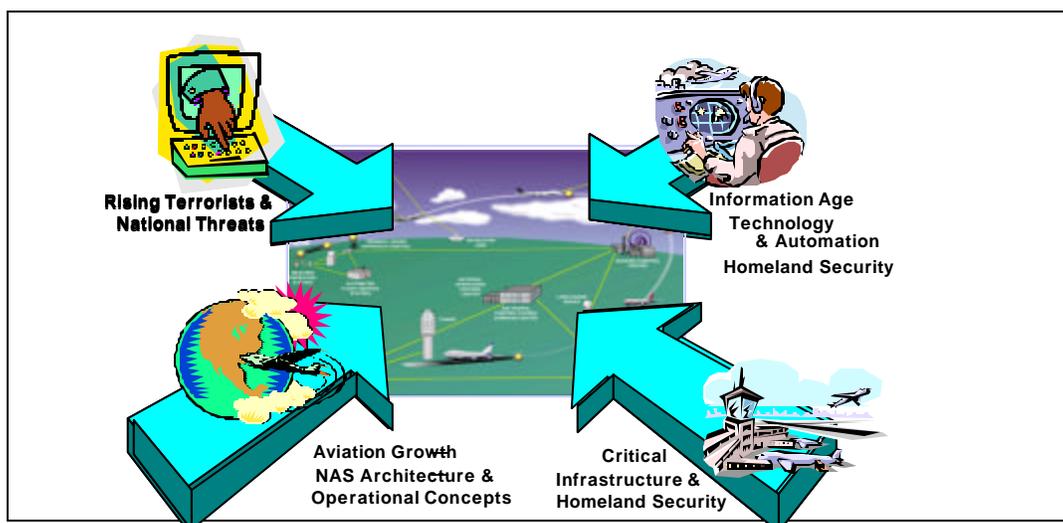


Figure 4.8.6-1. Force of Change Driving Security

These four factors drive the FAA toward 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.

**4.8.6.1.1 Information Security Engineering Principles**

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. NIST<sup>1</sup> SP 800-27 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 4.8.6-1, where one check (✓) signifies that the principle can be used to support the life-cycle phase, and two checks (✓✓) signify that the principle is key to successful completion of the lifecycle phase.

**Table 4.8.6-1. IT Security Principles (from NIST SP 800-27) Versus AMS Lifecycle**

IT Security Principles (NIST SP 800-27)		Mission Analysis		Investment Analysis		Solution Implementation	In-Service	Disposal
#	Description	Service Area Analysis	Concept and Requirements Analysis	Initial	Final			
1	Establish a sound security policy as the “foundation” for design.	vv	vv	v	v	v	v	v
2	Treat security as an integral part of the overall system design.	vv	vv	vv	vv	vv	vv	v
3	Clearly delineate the physical and logical security boundaries governed by associated security policies.	vv	vv	vv	vv	v	v	
4	Reduce risk to an acceptable level.	vv	vv	vv	vv	vv	vv	vv
5	Assume that external systems are insecure.	vv	vv	vv	vv	vv	vv	v
6	Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.	vv	vv	vv	vv		vv	
7	Implement layered security (Ensure no single point of vulnerability).	v	v	vv	vv	v	vv	v
8	Implement tailored system security measures to meet organizational security goals.	v	v	vv	vv	v	vv	v
9	Strive for simplicity.	v	v	vv	vv	v	vv	v
10	Design and operate an IT system to limit vulnerability and to be resilient in response.	v	v	vv	vv		vv	
11	Minimize the system elements to be trusted.	v	v	vv	vv	v	vv	

<sup>1</sup> The National Institute of Standards and Technology (NIST) is a nonregulatory 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.

IT Security Principles (NIST SP 800-27)		Mission Analysis		Investment Analysis		Solution Implementation	In-Service	Disposal
#	Description	Service Area Analysis	Concept and Requirements Analysis	Initial	Final			
12	<i>Implement security through a combination of measures distributed physically and logically.</i>			VV	VV	V	V	V
13	Provide assurance that the system is, and continues to be, resilient in the face of expected threats.	V	V	VV	VV	V	VV	V
14	Limit or contain vulnerabilities.			VV	VV	V	V	
15	Formulate security measures to address multiple overlapping information domains.	V	V	VV	VV	V	V	
16	Isolate public access systems from mission critical resources (e.g., data, processes, etc.).	V	V	VV	VV	V	V	
17	Use boundary mechanisms to separate computing systems and network infrastructures.			VV	VV	V	VV	
18	Where possible, base security on open standards for portability and interoperability.	V	V	VV	VV	V		
19	Use common language in developing security requirements.	VV	VV	VV	VV		VV	
20	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.	V	V	VV	VV	VV	V	
21	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.			VV	VV	V	VV	
22	Authenticate users and processes to ensure appropriate access control decisions both within and across domains.	V	V	V	V	V	VV	
23	Use unique identities to ensure accountability.	V	V	V	V	V	VV	
24	Implement least privilege.	V	V	V	V	V	VV	
25	Do not implement unnecessary security mechanisms.	V	V	VV	VV	VV	V	
26	Protect information while being processed, in transit, and in storage.	V	V	VV	VV	V	VV	V
27	Strive for operational ease of use.	V	V	VV	VV	V	VV	
28	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.	V	V	V	V	V	VV	
29	Consider custom products to achieve adequate security.	V	V	VV	VV	V	V	
30	Ensure proper security in the shutdown or disposal of a system.			V	V		V	

IT Security Principles (NIST SP 800-27)		Mission Analysis		Investment Analysis		Solution Implementation	In-Service	Disposal
#	Description	Service Area Analysis	Concept and Requirements Analysis	Initial	Final			
31	Protect against all likely classes of "attacks."	v	v	vv	vv	vv	v	v
32	Identify and prevent common errors and vulnerabilities.			vv	vv			
33	Ensure that developers are trained in how to develop secure software.	vv	vv	vv	vv	v		

Subsection 4.8.6.3 (below) illustrates how ISE principles apply to the acquisition process and system lifecycle, including establishment of system-level security policy and integration of security into system design, which are two NIST SP 800-27 principles. Reducing information security risk to an acceptable level is a primary ISE principle. In today's networked world, the concept of risk management is central to ISE. Security risk management includes assessment, mitigation, monitoring, and control of security risks throughout the system lifecycle. The FAA defines information security risk as follows:

**The combination of a threat, its likelihood of successfully attacking a system, and the resulting effects and harm from that successful attack.**

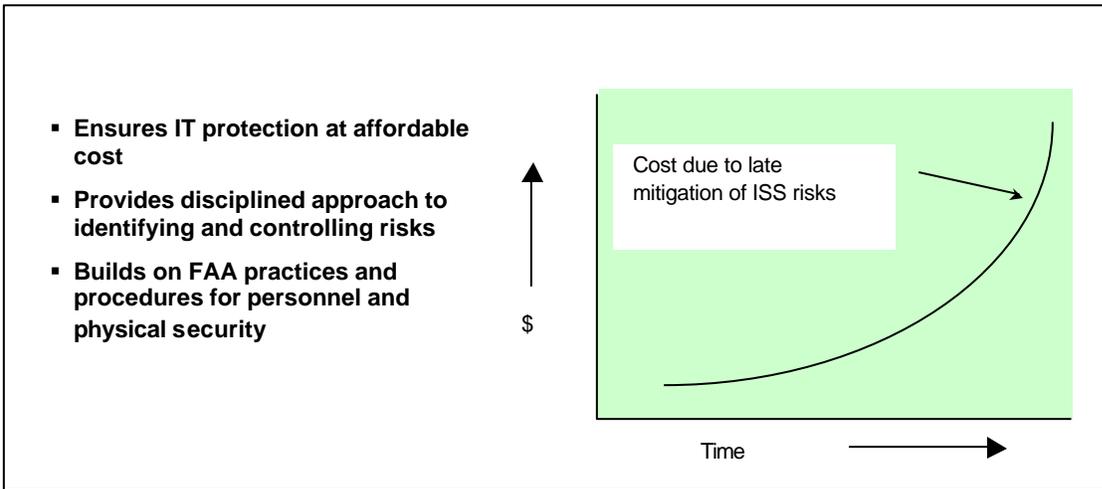
Based on FAA Order 1370.82, the appropriate Designated Approving Authority (DAA) determines the acceptable level of risk based on a carefully considered risk assessment. The DAA determines whether the benefit of operating/connecting the system outweighs the residual risk, which is defined as the combined 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 4.8.6-2 illustrates the benefit of early ISE involvement in the system lifecycle.



**Figure 4.8.6-2. Benefits of Early Information Security Engineering**

Security risk management applies to every AMS phase. Subsection 4.8.6.2 (below) integrates guidance from NIST SP 800-30, Risk Management Guide for Information Technology Systems into the FAA Risk Management process model (Section 4.10). Table 4.8.6-2 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 4.8.6-2. Integration of Information Security Risk Management Into AMS**

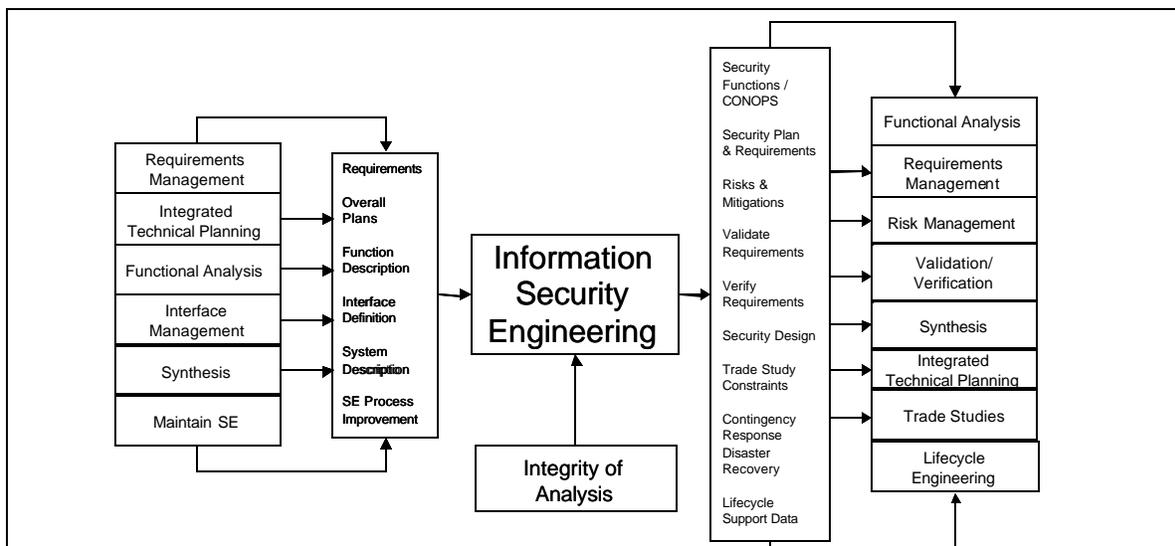
<b>NIST SP 800-30 Phases</b>	<b>FAA AMS Phases</b>	<b>Support From Risk Management Activities</b>
Phase 1 Initiation	Mission Analysis	Identified risks are used to support development of system requirements, including security requirements, and a security portion of the Concept of Operations (CONOPS).
Phase 2 Development or Acquisition	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.
Phase 3 Implementation	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.

NIST SP 800-30 Phases	FAA AMS Phases	Support From Risk Management Activities
Phase 4 In-Service Management	Late stages of Solution Implementation and In-Service Management, including Technology Refresh	Risk management activities are performed for periodic system recertification and reauthorization, or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces).
Phase 5 Disposal	Service Life Extension	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled, and that system migration is conducted in a secure and systematic manner.

**4.8.6.2 Information Security Inputs**

As Figure 4.8.6-3 shows, several SE elements 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 life-cycle. Subsection 4.8.6.4 (below) details the ISE outputs and products, while subsection 4.8.6.3 discusses the ISE products that result from applying the ISE principles.



**Figure 4.8.6-3. ISE Relationship to Other System Engineering Processes**

### 4.8.6.3 Information Security Engineering Process Tasks

The ISE process tasks support the phased AMS decisions, as shown in Figure 4.8.6-4. Each program or Service Organization shall tailor its ISE activities to meet its program milestones and use its System Engineering Management Plan (SEMP) to tailor its ISE activities and process tasks.

Each phase has ISE products that support the other SE elements, consistent with Figure 4.8-1, "Specialty Engineering Process-Based Management Chart," and subsection 4.8.0.3, "General Specialty Engineering Process Tasks" (in Section 4.8). The Information System Security Plan (ISSP) is a key ISE planning document for every FAA IT program. The ISSP provides an overview of the system, presents an approach for meeting associated security requirements, and delineates responsibilities and rules for controlling access and use of information and related assets within the system. The program ISSP is a living document, prepared early in the system lifecycle and updated regularly during program/system development. Table 4.8.6-4 summarizes the ISE process task alignment with the AMS phases.



**Legend**

**ISE Risk Management Process Aligned With AMS**

Numbered items correspond to AMS Lifecycle diagram numbers, above

- |   |  |
|---|--|
| a. Integrate Initial Security Needs and Threat Stipulation into MNS | h. Integrate Security Architecture and Design            |
| b. Develop Preliminary ISSP including Basic Security Policy         | i. Update ISSP   |
| c. Develop CONOPS and Preliminary Security Requirements             | j. Develop Security Test Plans and Procedures            |
| d. Develop Preliminary Vulnerability and Risk Assessment            | k. Develop Users Guides, Training, and Contingency Plans |
| e. Update Vulnerability and Risk Assessment                         | l. Conduct Security Testing                              |
| f. Update CONOPS and Security Requirements                          | m. Create Final Security C&A Documents                   |
| g. Integrate Security Requirements with System Requirements         | n. Obtain Security Authorization/Accreditation           |
|   | o. Prepare for Tech Refresh and Upgrade                  |

**Figure 4.8.6-4, ISE Process and the AMS Lifecycle Spiral**

The following subsections summarize the ISE tasks for each AMS phase.

#### **4.8.6.3.1 Mission Analysis Phase**

The ISE process starts in Mission Analysis. In this phase, the ISE process focuses on the proposed system's operating environment, system boundaries, information assets and functions, 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 1370.82, as well as from FAA operating procedures and instructions. Basic system security policy is the set of rules governing control, access, and use of system information. For example, a basic security policy statement may be that only authorized FAA users shall access the system. The ISE process applies Federal Information Processing Standards (FIPS) 199-1 to categorize system information assets and functions. The ISE process analyzes the system and NAS concept of operations (CONOPS) and mission need statement to formulate a basic security policy. The security planning aspects of ISE also begins in this phase, following guidance of NIST SP 800-18. Security requirements, based on security policy, are in the preliminary Program requirements document.

#### **4.8.6.3.2 Investment Analysis Phase**

Integrating the ISE process with SE elements is essential. During initial investment analysis, ISE develops and documents the security CONOPS and the initial security requirements for the initial Requirements Document. The investment analysis team uses the CONOPS and security requirements to evaluate system alternatives. Security engineers on the team conduct a preliminary risk assessment using updated threat and vulnerability data to determine specific risks that must be controlled/mitigated. Security trade studies are performed to evaluate system alternatives and to assess security risk controls/mitigation measures related to the system alternatives. Also, security trade studies identify native, existing system, and/or network features that reduce the likelihood of system threats successfully exploiting a vulnerability. These trade studies compare costs and benefits of system features/security controls in terms of risk reduction. Trade studies may evaluate the cost-effectiveness of different controls for a given risk or set of risks. Also, system alternatives may require different types of controls to balance system performance and security requirements against the security risks/costs of different alternatives. Different system alternatives may have significantly different physical and/or system architectures that would require different security controls, which lead to different security costs and effectiveness.

During the final stage of the Investment Analysis phase, ISE refines and updates the preliminary risk assessment. Updated threat and vulnerability data is applied, analyzing the costs and effectiveness of system features and security controls that are associated with each of the final system alternatives. ISE provides final security requirements for the final Program Requirements Document and the system specification, as well as special requirements for the Solicitation Information Request (SIR) and contract Statement of Work (SOW). In developing the final system requirements, ISE analyzes and establishes the appropriate assurance level to be proven during system implementation. Assurance in this context addresses the required level of confidence in the security function and performance and ensures that the security controls function in an integrated fashion. Assurance can be gained through many techniques, including conformance testing, independent verification testing, and employing diverse and/or redundant capability.

ISE shall support a documented agreement among FAA stakeholders regarding the necessity and sufficiency of the security requirements. Clearly documenting the agreement to security requirements before the Investment Decision becomes the foundation for the Security Certification and Authorization Package, which shall be completed before the In-Service

Decision. During the investment analysis, ISE identifies the technically qualified, senior FAA official who shall certify that the system security controls meet the minimum FAA/NAS ISS requirements (see DAA discussion in 4.8.6 above). The ISSP, which was based on NIST SP 800-18 and was a conceptual draft during the Mission Need phase, is updated to become an initial draft.

The ISE products from this phase include the updated preliminary risk assessment, final security requirements, security trade studies to support cost-benefit/investment analysis of security controls, and input to the SIR, SOW, system specification, and Contract Data Requirements List (CDRL) for systems to be acquired. These products support the AMS milestone decision for transition into the Solution Implementation phase.

#### **4.8.6.3.3 Solution Implementation Phase**

The ISE activities during earlier phases provide the basis for updating, monitoring, and controlling system security risks and the respective mitigation measures or controls that are implemented during this phase of system development. A summary of ISE activities for this phase includes the following:

- Revise the security CONOPS and security requirements based on functional analysis performed during early stages of the Solution Implementation phase.
- Analyze the physical/system architecture, resulting in an allocation of the security features to be implemented in the system under development. Security trade studies may be needed to identify the appropriate security controls to be implemented that balance system and security requirements.
- Integrate the security features into the security architecture to balance them with the system architecture and design. Security trade studies, interface security requirements, and other SE outputs contribute to successful integration of security architecture into system design. System design reviews are key milestones for ensuring that security controls are integrated into system development.
- Update the ISSP based on the expected ISS functional and assurance controls derived from the system architecture and design. Refine system test planning and procedures to ensure that all security requirements and controls are addressed. The ISSP supports Validation (Section 4.12, subsection 4.12.1) and Synthesis (Section 4.5) to assess controls and assurance as being cost effective and meeting the ISS requirements. Use Risk Management (Section 4.10) and Requirements Management (Section 4.3) to mitigate security risk to acceptable levels. The criticality/sensitivity of the system and its information assets guides the type and level of controls and testing.
- Develop a users guide, training plans, and contingency/disaster recovery plans. Security procedures, rules, training, and planning for contingency and disaster recovery operations may be integrated into the integrated logistics support and lifecycle planning for systems.
- Conduct security testing. Security controls and mechanisms may be tested incrementally and as a part of system development testing. For mission-critical systems, a third party shall conduct independent testing of system vulnerabilities.
- Create final security Certification and Authorization (C&A) documents. The results of ISE activities—including relevant results from related SE elements such as Integrated Technical Planning (Section 4.2), Synthesis (Section 4.5), Validation and Verification (Section 4.12), and Lifecycle Engineering (Section 4.13)—shall be

considered as final security C&A documents. The Air Traffic Organization provides templates for collecting and presenting C&A documentation.

#### **4.8.6.3.4 In-Service Management Phase**

Activities during this phase include the following:

- Obtain security C&A. Stakeholder C&A review shall ensure that the DAA is in a position to certify and authorize the system as meeting security requirements and as presenting an acceptable risk to the FAA mission and NAS operations.
- Conduct performance measurement, monitoring, and reporting of security controls and incidents. Ensure that monitoring of ISS performance and assurance for the respective NAS service/capability has not degraded and that new vulnerabilities have not been introduced to the operational system.
- Update the C&A package to reflect any major configuration changes at least every 3 years, assessing changes in the environment and system for previously unforeseen risks from new threats and vulnerabilities. Plan and take corrective action as necessary.
- For disposal of the system, the following types of activities may be addressed in the Information System Security Plan, and conducted at the appropriate stage of the System Development Lifecycle
  - Archive Information—retain information as necessary, keeping in mind legal requirements and future technology changes that render the retrieval method obsolete.
  - Sanitize Media—ensure data is deleted, erased, or written over as necessary.
  - Dispose of Hardware and Software—dispose of the hardware and software in accordance with ISS policy.

Table 4.8.6-3 relates the required C&A package to the ISE process steps that provide the conceptual, initial, draft, update, and final results for the C&A package.

**Table 4.8.6-3. Security Certification and Authorization Documents Related to Information Security Engineering Process**

<b>SCAP Documentation</b>	<b>ISE Process Source</b>	<b>How To Reference</b>
System Characterization	ISE h, Draft ISE i, Draft	Security Risk Assessment Methodology and System Characterization Template
Information System Security Plan	ISE b, Conceptual ISE d, Draft ISE i, Update ISE m, Final	Security Risk Assessment Methodology and ISSP Template
Risk Assessment Report (Includes Threat and Vulnerability Assessments)	ISE d, Initial ISE e, Update ISE m, Final	Security Risk Assessment Methodology and Risk Assessment Report Template
Security Test Plan and Test Results Report	ISE e, Initial ISE g, Draft ISE j, Update ISE m, Final	Security Risk Assessment Methodology and Security Test Plan and Test Results Template
Risk Mitigation/Remediation Plan	ISE i, Draft ISE m, Final	Security Risk Assessment Methodology and Risk Mitigation/Remediation Plan Template
Contingency/Disaster Recovery Plan	ISE i, Initial ISE k, Draft ISE m, Final	Security Risk Assessment Methodology and Contingency/Disaster Recovery Plan Template
Executive Summary	ISE i, Draft ISE m, Final	Security Risk Assessment Methodology and Executive Summary Template
C&A Certificate	ISE i, Draft ISE m, Final	Security Risk Assessment Methodology and C&A Statement Template

**4.8.6.4 Information Security Engineering Outputs/Products**

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.

**4.8.6.4.1 Information System Security Plan (ISSP)**

The system owner (Information Systems Security Certifier) or Service Level Mission Need (SLMN) sponsor shall initiate the ISSP during mission needs 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 4.8.6-4 relates the ISE activities and products to both the AMS milestone products and SE products. Analysis products outlined in subsection 4.8.6.4.2 below are used to update the ISSP.

Table 4.8.6-4. Acquisition Management, System Engineering, and Information Security Engineering Relationship

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 4.8.6-4)	ISE Output/Product	AMS and SE Elements/Products Affected
Initial requirements, Initial functional architecture, Threat analysis criteria, OSA	ISE a. Integrate Initial Security Needs and Threat Stipulation into the SLMN	Statement of security policy and threat environment stipulation	<ul style="list-style-type: none"> <li>• New/updated SLMN</li> <li>• Draft pPR, including the concept of use;</li> <li>• Initial investment analysis plan</li> <li>• System Investment Analysis Review</li> </ul> Requirements Management, Functional Analysis, Synthesis
CONOPS, Initial requirements, analysis criteria, OSA	ISE b. Develop CONOPS and Preliminary Security Requirements	Initial Security requirements, CONOPS	<ul style="list-style-type: none"> <li>• Business case analysis report</li> <li>• Updated pPR for each alternative under serious consideration</li> <li>• Initial investment analysis plan</li> <li>• Acquisition strategy in the ISAP for each alternative under serious consideration</li> </ul> Requirements Management, Functional Analysis, Conceptual functional architecture, Synthesis, ITP
FAA Policy, Standards, NAS Architecture, OSED, CONOPS	ISE c. Develop Preliminary ISSP (Including Basic Security Policy)	Preliminary ISSP with security policy statement	<ul style="list-style-type: none"> <li>• Final SLMN</li> <li>• CONOPS</li> <li>• Final Investment Analysis Plan</li> <li>• Initial description of alternatives</li> </ul> Requirements Management, Functional Analysis, RVCD, Trade Studies, Interface Management, SEMP

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 4.8.6-4)	ISE Output/Product	AMS and SE Elements/Products Affected
CONOPS, Initial Functional Architecture, Functional Specification, Interface Control Documents, Initial VRTM, Stakeholder Needs	ISE d. Develop Preliminary Vulnerability and Risk Assessment	Preliminary Vulnerability and Risk Assessment	<ul style="list-style-type: none"> <li>• fPR</li> <li>• Final investment analysis report</li> <li>• Final Exhibit 300</li> <li>• Final ISAP</li> </ul>
			Requirements Management, RVCD, VRTM, OSED, Specialty Engineering, Risk Management, Validation, SEMP
CONOPS, Initial Functional Architecture, Functional Specification, Interface Control Documents, Initial VRTM, Stakeholder Needs	ISE e. Update the Vulnerability and Risk Assessment	Updated Vulnerability and Risk Assessment	<ul style="list-style-type: none"> <li>• SIR</li> <li>• System Specification</li> <li>• SOW</li> <li>• CDRL</li> <li>• Source selection criteria and plan</li> </ul>
			Requirements Management, Specialty Engineering, Risk Management, Validation
CONOPS, Initial requirements, analysis criteria, OSA	ISE f. 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, Security concept of use	ISE g. Integrate Security Requirements with System Requirements	Initial Verification Requirements Traceability Matrix, Interface Requirements Documents	<ul style="list-style-type: none"> <li>• System Requirements Review</li> <li>• System Design Review – PDR</li> </ul>
			Requirements Management, Integrated Technical Planning, Trade Studies, Synthesis, Interface Management, Configuration Management, Risk Management

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 4.8.6-4)	ISE Output/Product	AMS and SE Elements/Products Affected
Physical Architecture, Final Security Requirements, Design Analysis Report, Functional Architecture	ISE h. Integrate Security Architecture and Design	Updated Physical Architecture, Functional Architecture	<ul style="list-style-type: none"> <li>• System Design Review — CDR</li> <li>• System Capability Demonstration</li> </ul>
			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	ISE i. Update the ISSP	Updated Information System Security Plan	<ul style="list-style-type: none"> <li>• ISAP</li> <li>• Integrated Lifecycle Plan</li> <li>• System Test Plan</li> <li>• OT&amp;E Plan</li> </ul>
			ITP, Specialty Engineering, Configuration Management, Lifecycle Engineering
Verification Requirements, Traceability	ISE j. Develop Security Test Plans and	Security Test Plan, Security Test Procedures	<ul style="list-style-type: none"> <li>• System Test Plan</li> <li>• OT&amp;E Plan</li> </ul>

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 4.8.6-4)	ISE Output/Product	AMS and SE Elements/Products Affected
Matrix, Risk Mitigation Plans, Interface Control Documents, Test and Assessment Articles, Physical Architecture, Functional Architecture, Functional Specification, Master Verification Plan	Procedures		<ul style="list-style-type: none"> <li>• Integrated Technical Planning, Requirements Management, Interface Management, Verification, RVCD, VRTM</li> </ul>
Trade Study Reports, Operational Services and Environmental Description, Functional Specification, Government and International Regulations and Statutes, FAA Policy, Requirements	ISE k. Develop User's Guides, Training, and Contingency Plans	Contingency and Disaster Recovery Plan, User's Guides, Security Awareness Training (see 4.14)	<ul style="list-style-type: none"> <li>• Integrated Lifecycle Plan</li> <li>• Functional Configuration Audit</li> <li>• Physical Configuration Audit</li> </ul> <p>Functional Analysis, Configuration Management, Trade Studies, Specialty Engineering, Verification, ITP</p>
Updated Verification Requirements Traceability Matrix,	ISE l. Conduct Security Testing	Updated Risk Mitigation Plan, Security Test Report	<ul style="list-style-type: none"> <li>• Test Readiness Review</li> <li>• Qualification Test</li> <li>• Final Acceptance Test</li> <li>• Site Acceptance Test</li> </ul>

AMS/SE Input	ISE Security Risk Management Activities (Refer to Figure 4.8.6-4)	ISE Output/Product	AMS and SE Elements/Products Affected
Requirements Verification Compliance Document, Verification Criteria, Updated Master Verification Plan			Verification, Integrated Technical Planning, Requirements Management, Configuration Management, Risk Management
Risk Mitigation Plan, Program Risk Summary, Updated ISSP, Contingency Plans, Test Validation Reports,	ISE m. Create Final Security C&A Documents	Certification Package	<ul style="list-style-type: none"> <li>• In-Service Review Checklist</li> <li>• OT&amp;E Report</li> </ul> Specialty Engineering, Configuration Management, Synthesis, Risk Management
Certification Package, FAA Management Decisions, Government and International Regulations and Statutes	ISE n. 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	ISE o. 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

#### 4.8.6.4.2 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 4.8.6-5 indicates the type of closed-loop security risk management that is applied during the AMS phases consistent with FAA ISS Policy Order 1370.82.

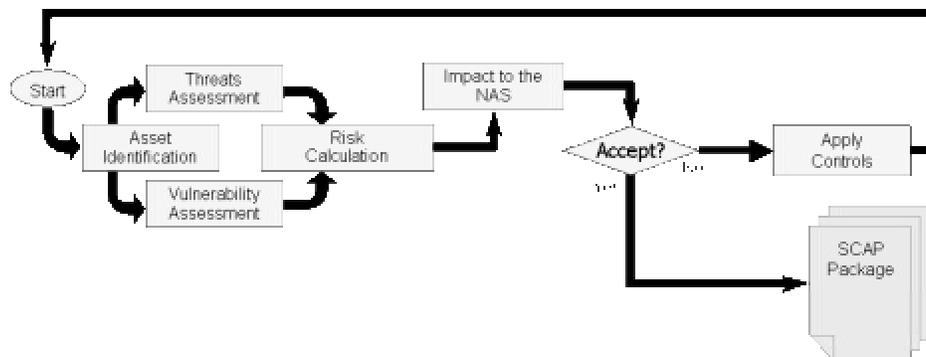
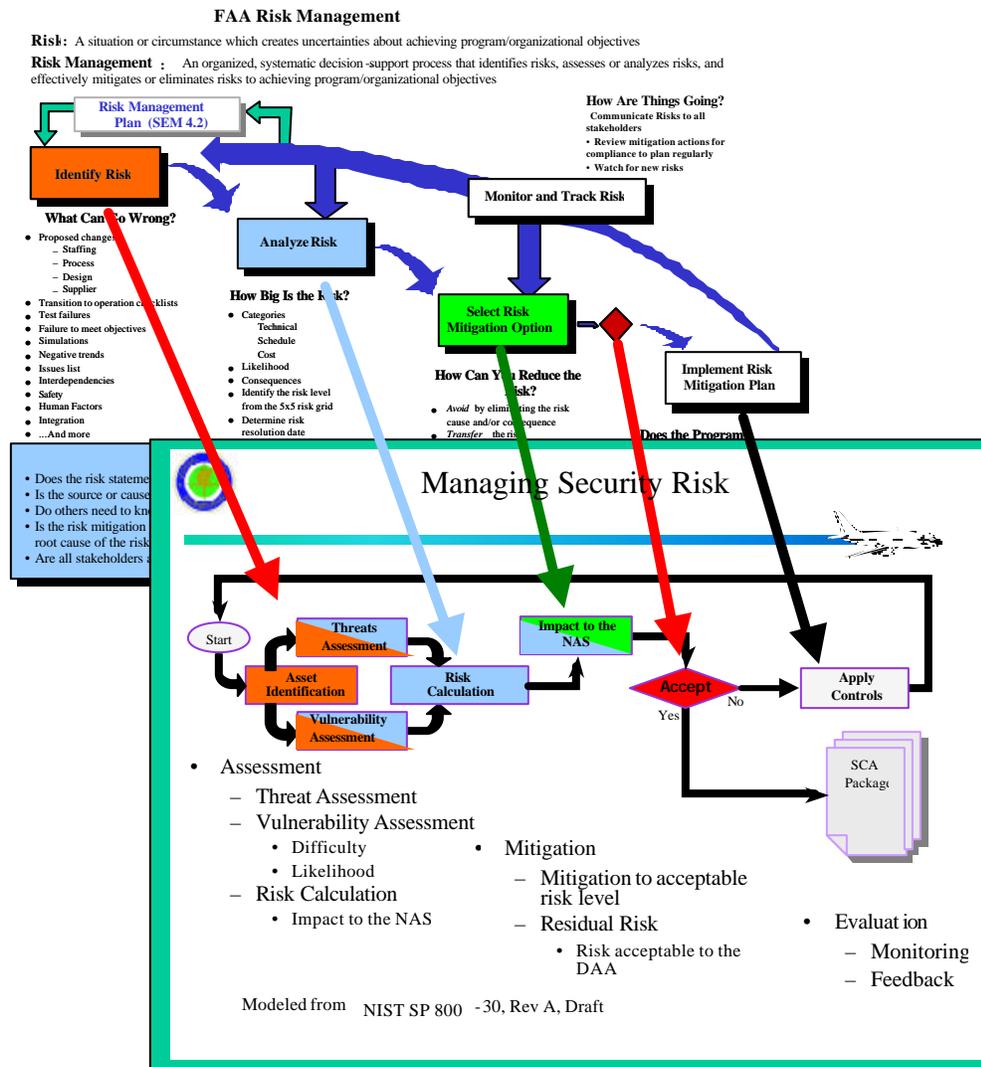


Figure 4.8.6-5. Closed-Loop Security Risk Management

This closed-loop method of risk management supports the FAA risk management process model described in Risk Management (Section 4.10), as shown in Figure 4.8.6-6 below.



**Figure 4.8.6-6. Correlation of Information Security Methodology With FAA Risk Management Model**

The ISE Risk Assessment Matrix (Figure 4.8.6-7) 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.

Impact

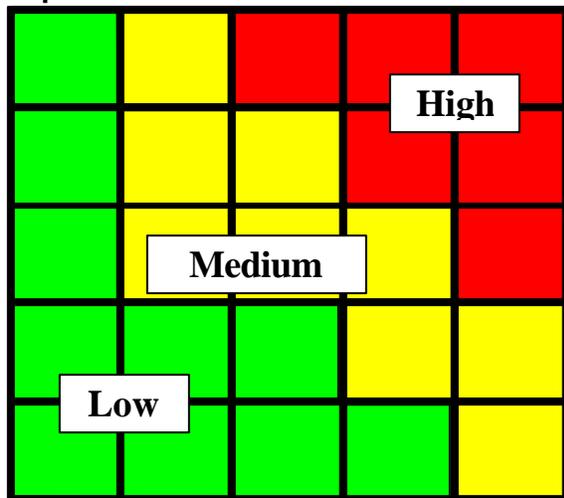


Figure 4.8.6-7. ISE Risk Assessment Matrix

#### 4.8.6.5 Information Security Engineering Tools

There is not one 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.

#### 4.8.6.6 Information Security Engineering Metrics

Reserved.

#### 4.8.6.7 References

1. Clinger-Cohen Act of 1996.
2. FAA Order 1370.82, *Information Systems Security Program*.
3. Federal Information Security Management Act (FISMA) of 2002.
4. FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*.
5. FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*.
6. NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*.
7. NIST Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*.
8. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*.
9. OMB Circular A-130, *Management of Federal Information Resources*.
10. OMB Circular A-130, *Appendix III, Security of Federal Automated Information Resources*.

## **4.8.7 Hazardous Materials Management/Environmental Engineering**

Hazardous Material Management/Environmental Engineering (HMM/EE) is the subset of Specialty Engineering concerned with the impacts of both the program on the environment and the environment on the program. Federal, state, and local environmental agencies have established mandates that regulate program impacts on the environment. These mandates include requirements to manage hazardous materials and to safeguard natural resources including ambient air, water, and land-based resources. FAA orders and directives (e.g., FAA Order 1050.10, Prevention, Control, and Abatement of Environmental Pollution at FAA Facilities) relate Federal environmental regulations to FAA activities and also provide additional environmental 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 within SE.

### **4.8.7.1 What Is Hazardous Material Management/Environmental Engineering?**

HMM/EE is the mechanism applied within the SE process to ensure a program's ongoing compliance with applicable environmental laws. HMM/EE is also the SE process designed to provide early, predeployment planning and coordination to minimize the negative impacts that site-specific environmental conditions may have on a program's operability. Compliance with various environmental regulations is required throughout a program's lifecycle, requiring early and continuous application of HMM/EE principles.

Key considerations are pollution prevention, safety and health (including system safety), cultural and natural resource conservation, public participation, and energy and water conservation. It is recommended that additional issues concerning the applicability of state and local agency requirements to federal agencies be referred to the legal office for an evaluation of supremacy clause and sovereign immunity implications. For example, the National Environmental Policy Act requires preparation of an environmental assessment for all proposed federal actions that are not categorically excluded.

Additionally, the Resource Conservation and Recovery Act delineates 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. Through HMM/EE, the breadth of environmental requirements are continuously monitored and considered to ensure that FAA's programs take the steps to maintain compliance.

HMM/EE processes also highlight the impacts that environmental conditions and site-specific characteristics may have on a program. FAA specifications developed for various types of equipment 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 adhered to in the SE process to ensure the reliability of systems fielded under unique environmental settings.

### **4.8.7.2 Why Perform Hazardous Material Management/Environmental Engineering?**

HMM/EE is performed to:

- Support reliable, safe, and sustained NAS operations
- Ensure that compliance with FAA, federal, state, and local environmental requirements
- Ensure environmental considerations are included in the acquisition management process
- Track the status of environmental issues with new and existing systems
- Minimize cost and schedule risks through early detection of environmental issues

Through various regulations, such as FAA Order 1050.17, Airway Facilities Environmental and Safety Compliance Program, the FAA has mandated and delineated requirements to comply with applicable environmental regulations. The FAA Acquisition Toolset System (FAST) ensures that these regulations are considered in the acquisition process in AMS Section 2.9.8, Environmental, Occupational Safety and Health, and Energy Considerations:

*FAA acquisitions are subject to federal environmental, occupational safety and health, and energy management statutes, regulations, executive orders, and Presidential memoranda. Key considerations are pollution prevention, safety and health (including system safety), cultural and natural resource conservation, public participation, and energy and water conservation. Additional issues concerning the applicability of state and local agency requirements to federal agencies should be referred to the legal office for an evaluation of supremacy clause and sovereign immunity implications.*

The following illustrate some of the requirements:

- The National Environmental Policy Act “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, the FAA may make a decision on the federal action.”
- Various other environmental laws (e.g., the Federal Facilities Compliance Act) “impose environmental requirements, and sanctions for noncompliance, including civil penalties.”
- The Occupational Safety and Health Administration (OSHA) “requires a safe and healthful workplace for all employees, and compliance with OSHA standards.”

*OSHA (29 CFR §1910.28) 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.*

- The National Energy Conservation Policy Act “requires energy and water conservation measures for federal buildings, facilities or space.”

*Environmental, safety and health, and energy conservation considerations apply from the beginning of the acquisition lifecycle 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 identifies applicable environmental requirements to include in development and acquisition of new systems, thereby providing significant savings through risk minimization, cost avoidance, and enhancement of system efficiency. Additionally, consideration of environmental impacts on systems while they are in the developmental stages ensures their functionality in various field conditions.

HMM/EE conducted as part of in-service program management analyzes the impact that engineering changes in the field may have on environmental concerns. As obsolete equipment is removed, HMM/EE ensures that replacement equipment complies with applicable environmental regulations. In particular, decommissioning and removal of obsolete equipment require HMM/EE considerations to ensure that final disposition/disposal is conducted in accordance with applicable environmental requirements. HMM/EE also evaluates the impact that regulatory changes may have on fielded systems.

Programs that fail to fully incorporate HMM/EE principles may have significant impacts on NAS operations. Noncompliant programs may:

- Be removed from service through regulatory enforcement actions
- Require costly post-fielding/retrofit modifications
- Incur fines

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.

#### **4.8.7.3 Hazardous Material Management/Environmental Engineering Process Tasks**

HMM/EE follows the process tasks outlined in General Specialty Engineering Process Tasks (subsection 4.8.0.3).

#### **4.8.7.4 Hazardous Material Management/Environmental Engineering Outputs and Products**

Throughout the various phases of the system acquisition process, HMM/EE is used in developing and reviewing key documents. Early implementation of HMM/EE principles is essential to minimize the impact that environmental requirements may have on system costs and operations. During the preliminary activities, such as development of mission needs, requirements, and investment analysis, HMM/EE is used to make initial assumptions and estimates on how environmental considerations may come into play throughout the various lifecycle stages.

During the solution implementation phase of the acquisition process, HMM/EE is used to shape portions of the SOW and system specifications documents as they relate to environmental considerations. For example, SOWs may be developed to support FAA efforts to meet National Environmental Policy Act demands that federal agencies minimize use of toxic substances in its operations.

During the in-service management phase of the system lifecycle, HMM/EE is 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 in mind may require corrective measures to meet environmental regulations. Additionally, the set of ever-changing environmental regulations may impact the way systems are operated. Finally, as old systems are decommissioned, HMM/EE is necessary to ensure that all disposal actions consider applicable environmental laws.

#### **4.8.7.4.1 Program Integration**

As part of the SE process, HMM/EE provides expertise for developing various documents required for program integration. Throughout the various lifecycle phases, HMM/EE ensures that all applicable regulations and environmental conditions are properly addressed so that their impacts are accounted for appropriately. For example, HMM/EE 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's role in developing IPPs, SOWs, Disposition/Disposal Plans, and other such documents generates comments and input concerning the compliance requirements that may impact the progress of program implementation, and FAA's compliance status and future liabilities.

Included in the HMM/EE aspects of program integration is a functional analysis of the OSED (see Section 4.4 (Functional Analysis)). 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 4.8.7-1 depicts HMM/EE Inputs and Outputs.

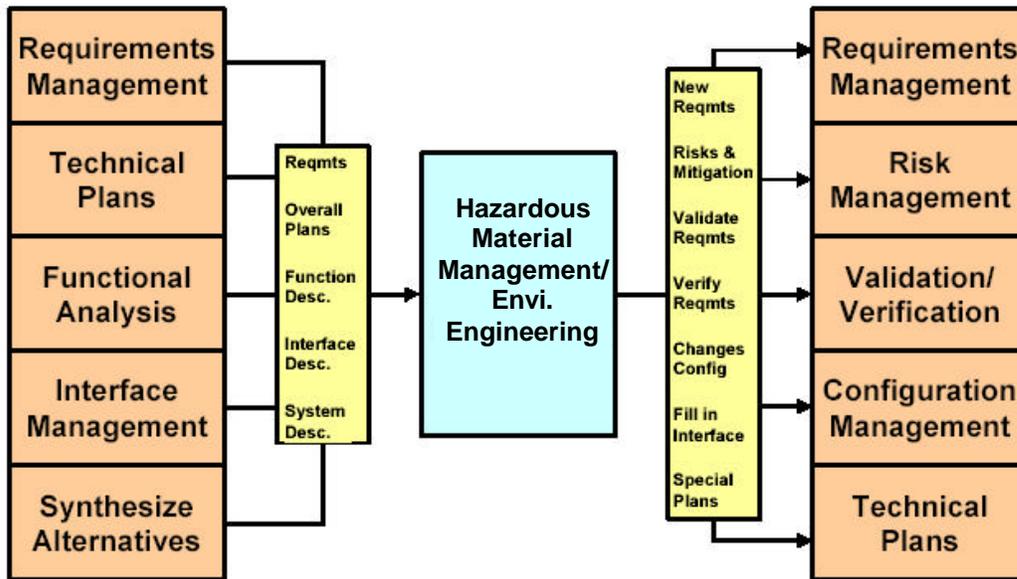


Figure 4.8.7-1. HMM/EE’s Relationship to Other System Engineering Processes

#### 4.8.7.4.2 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 FAA 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 to FAA Order 1050.17, FAA Order 4200.2, Utilization and Disposal of Excess and Surplus Personal Property, and AMS Section 2.8, Removing an Obsolete Solution, 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 subsection 4.2.2.1, “Introduction to the Integrated Program Plan”, in Section 4.2, Integrated Technical Planning.

#### 4.8.7.4.3 Products

Additionally, it is recommended that, through the HMM/EE process, a program have the capability to produce an inventory of the hazardous materials 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

- Supporting disposition/disposal efforts when obsolete equipment is removed from service

#### 4.8.7.5 References

1. *Airway Facilities Environmental and Safety Compliance Program*. FAA Order 1050.17. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.
2. *Utilization and Disposal of Excess and Surplus Personal Property*. FAA Order 4200.2. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.
3. *Removing an Obsolete Solution*. FAA Acquisition Management System, Section 2.8. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC. <http://fast.faa.gov/>.
4. *Prevention, Control, and Abatement of Environmental Pollution at FAA Facilities*. FAA Order 1050.10C. U.S. Department of Transportation, Federal Aviation Administration, Washington, DC.

## 4.9 Integrity of Analyses

### 4.9.1 Introduction to Integrity to Analyses

**Analysis is defined as a logical examination or study of a system to determine the nature, relationships, and interaction of its parts and environment.** Analysis emphasizes baseline system performance and/or compares development, production, or usage alternatives. Analysis is performed throughout the entire product lifecycle to support program decisions, encompassing technical performance and system acquisition considerations. Specific analyses are used throughout the System Engineering (SE) process. Analyses conducted to support a program may only add value if the results are credible, useful, verifiable, and sufficient.

Analysis, as described here, encompasses a broad range of perspectives. The nature of the system dictates that analysis may be performed relative to the entire system (or its subsets), the system's interaction with other systems, and/or the environment in which the system operates. Analysis may focus on the operational, functional, or physical aspects of the system and its interfaces. Analyses may range from the simple to the complex, quantitative to qualitative, top-down to bottom-up, and basic formulas to sophisticated simulations. Some specific scenarios that require analyses include:

- Exploring system concepts regarding viability and technology maturity
- Determining operational system requirements and measures of system merit
- Determining key system performance relationships to cost and other acquisition parameters
- Evaluating key system quality factors, including reliability, readiness, and maintainability
- Evaluating potential changes to improve performance, reduce cost, and so on
- Assessing risks and potential risk mitigation options
- Synthesizing allocated requirements into an acceptable physical design
- Evaluating specific physical designs (components and interfaces)
- Determining system characteristics before building or integrating the system
- Verifying system, subsystem, and component performance at various stages
- Monitoring production quality
- Diagnosing observed or perceived system deficiencies
- Evaluating produced and fielded system performance
- Evaluating processes used to support and achieve results

To ensure credible, useful, verifiable, and sufficient data/results for program management's decision-making process, the integrity and fidelity of various analyses performed on a program shall be understood and validated. This validation takes several forms: through the attributes of the tool suite (subsection 4.9.3.2), the proficiency and skills of the analyst (subsection 4.9.3.3), and the validity of the input data (subsection 4.9.3.4). The actual analyses performed are described in the other sections of this manual. The Integrity of Analysis process supports the other SE processes and is intended to provide a disciplined framework for conducting any required analysis, whether technical, programmatic, or administrative in nature. An Analysis

Management Plan that outlines the details of the various analysis methods and tools is either generated or incorporated into the System Engineering Management Plan (SEMP). It is recommended that this planning effort reflect the available inputs and program constraints regarding technical capabilities, schedule requirements, and cost requirements.

A wide range of tools may support analysis, including a spacecraft facility, wind tunnel, manned aircraft simulator, iron bird, computational model, physical model, computer-aided design model, spreadsheet, photograph, or paper and pencil. The analysis methods used, including tools, shall provide the required level of fidelity in representing the system or subsystem and any associated interfaces. The selected analysis method may be quantitative or qualitative or both. The common feature of all tools is that the tools are approximations of the system being analyzed. The level of fidelity achieved is one of the primary features that often sets one tool apart from another tool.

**Integrity of Analyses is defined as 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.** Competent users who iteratively apply a validated set of tools to a clearly defined data set ensure integrity. The Integrity of Analyses process (Figure 4.9-1) identifies the following tasks that shall be performed to ensure integrity:

- For each analysis, identify objectives, level of detail, and degree of validation required
- Select and/or develop the tools to meet the identified needs
- Ensure availability of analysts proficient in using the selected tools
- Ensure availability of proper and correct input data for each analysis conducted
- Perform analysis (reference task; see the SE element performing the actual analysis)
- Verify that analysis results are credible, useful, and sufficient

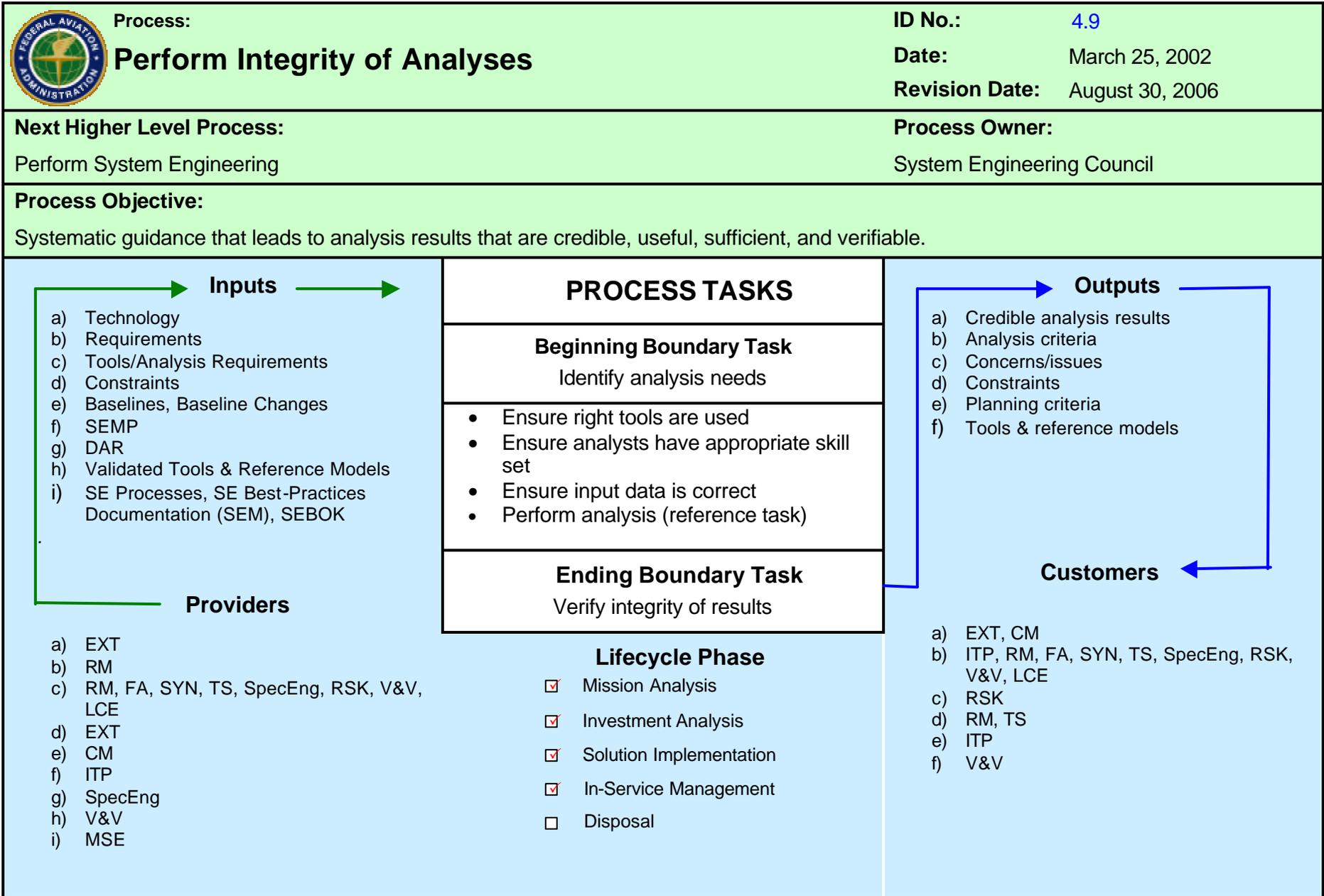


Figure 4.9-1. Integrity of Analyses Process-Based Management Chart

#### 4.9.1.1 Purpose

The Integrity of Analyses process provides systematic guidance that leads to analysis results, including the following:

- **Credible.** Results are valid and their implementation is feasible.
- **Useful.** Results align with their intended use in the program decision-making process.
- **Sufficient.** Quantity and quality are appropriate to properly aid decision making without performing excessive analysis
- **Verifiable.** Results are accompanied by a methodology, rationale, and traceability that produce an appropriate confidence level in the results.

Executing the process tasks identified in Figure 4.9-1 results in selecting the required analysis methods, performing the analysis, and verifying the results.

The initial selection of the method, tools, or model to be used in an analysis focuses on finding a practical tool that provides the most visibility into the problem with the least complexity. The process is implicitly iterative and is used across the program throughout its lifecycle. Because the process is iterative, there is an ongoing need to use the best approach to select the right method, tool, or model, considering the preferences of the stakeholders and other teams' previous experience with different tools. In addition, the limitations of budgets, technology, and schedule shall be evaluated. The bottom line is to have controls in place that guard against mistakes and embed a consistent level of confidence in the integrity of the analysis. The analysis, in turn, contributes significantly to the success of the decision-making processes of program management, teams, stakeholders, and contract managers. This result is achieved by addressing the methods of analysis to be used, attributes of the toolset, quality of the workmanship, and validity of the input data. The following subsections define the tasks that need to be completed to achieve analysis with integrity. Figure 4.9-2 illustrates the process tasks as well as the interactions between the Integrity of Analyses process with other SE elements.

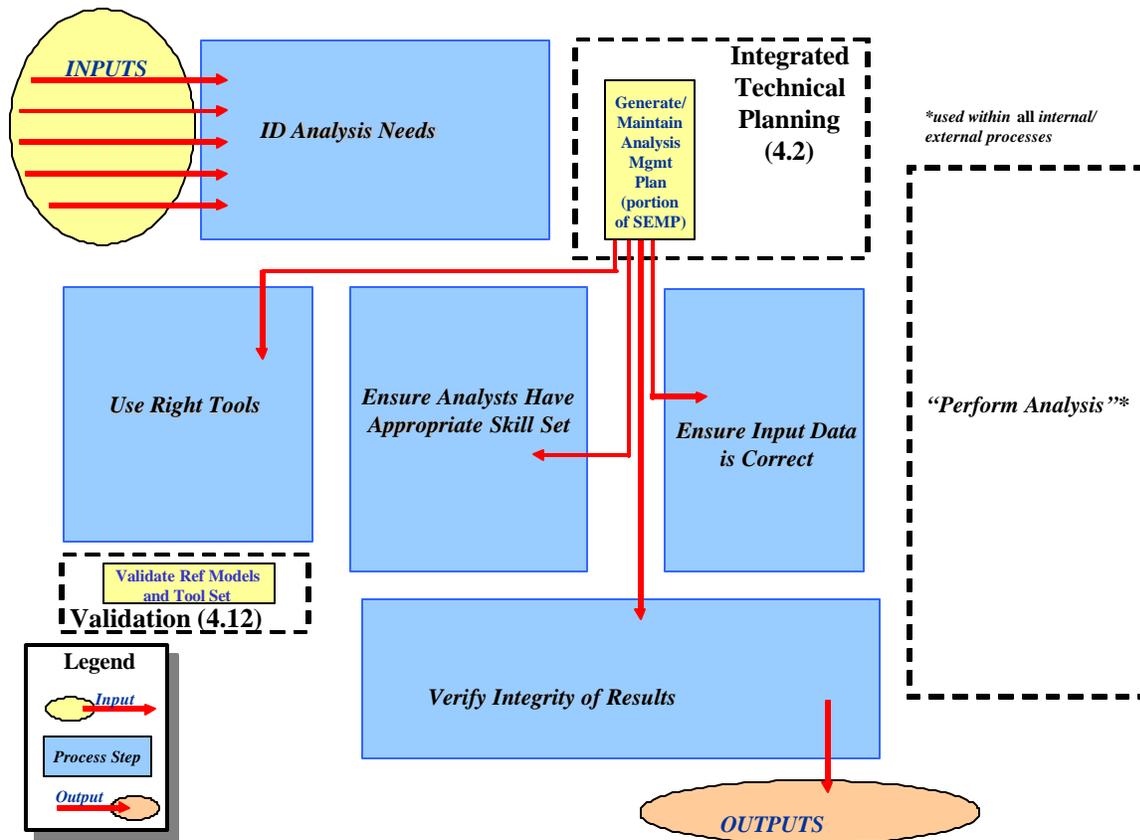


Figure 4.9-2. Integrity of Analyses Process

#### 4.9.2 Inputs to Integrity of Analyses

**Technology.** Technology insertion determines the methods and tools employed for various analyses. The degree of technology insertion is driven by schedule and economic factors.

**Requirements.** These requirements are defined to the extent that the results of a given analysis support a programmatic decision, whether driven by technical, cost, or schedule. The requirements are generated from customer, internal, or supplier sources and may be expressed textually or as models.

**Tools/Analysis Requirements.** The various process elements discussed in Integrated Technical Planning (Section 4.2) that perform analyses provide the requirements for tools and analysis for the project, which are constrained by program technical, schedule, and cost requirements and plans imposed by project management. These requirements are typically reflected in the planning information developed under Integrated Technical Planning.

**Constraints.** The analysis needs are frequently a balance between the desires and costs of analytic excellence (usually championed by the analysts) and the program's cost/risk/benefit constraints, which are usually reflected in the program's budgets, schedules, and goals.

**Baselines.** This data set defines the aspect of the system being modeled or analyzed and is under configuration control to the extent that all elements of the program are using the same baseline.

**Analysis Management Plan (AMP).** As part of the SEMP or as a stand-alone plan, the AMP contains the planning effort for the right tools, data, and analyst skill set (Figure 4.9-3). The AMP is developed and maintained under the Integrated Technical Planning process (Section 4.2).

**Analysis Reports.** An analysis is performed to provide an answer to a question. The analysis is credible only if it actually answers the question asked. Simulated results are not expected to precisely replicate results from the simulated systems. Additionally, analysis results may not be consistent among themselves. Analysis results are meaningless without description of the analysis method and the assumptions that generated those results.

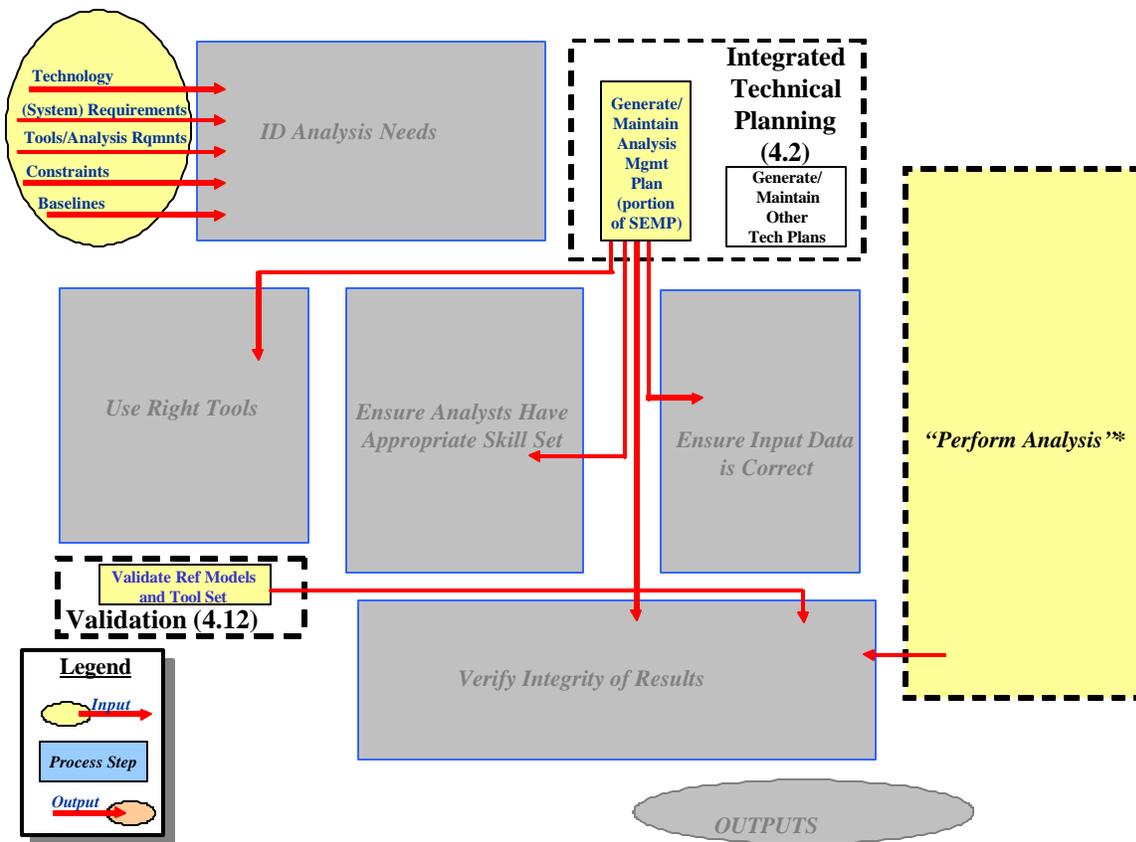


Figure 4.9-3. Integrity of Analyses Process Inputs

### 4.9.3 Integrity of Analyses Process Tasks

#### 4.9.3.1 Task 1: Identify Analysis Needs

As indicated by the definition in the introduction of this section, analysis is used to investigate system structure or behavior. The analysis results form a decision aid that emphasizes certain

aspects of system structure or performance in a limited number of architectures or configurations. Analyses are performed for a variety of specific needs relative to the system's lifecycle. For an analysis to be truly effective, the analysis results shall be closely aligned with the expressed needs and the decisions that the analysis is designed to support. It is good engineering practice to identify and plan around these needs. It is recommended that specific analysis needs be identified in the following areas:

- **Understand the various perspective(s)** to aid in decision making (e.g., system users, acquirers, builders, testers, and suppliers). Analysis results shall address stakeholder requirements and be capable of undergoing translation to address different stakeholder perspectives.
- **Codify objectives, requirements, and constraints** for the analysis itself and for managing the analysis. This includes using appropriate case definition and acceptable analysis products, as well as criteria that ensure suitability and effectiveness of the analysis when the analysis is complete. It is recommended that a concerted effort be made to identify which requirements are firm or soft and what conditions enable change.
- **Obtain sufficient system and environmental definition** to conduct the analysis cases. This includes defining analysis boundaries, necessary assumptions, rationale, frequency and depth of analysis, interactions required with other analyses, and capabilities of the toolset.
- **Identify control and decision points** to manage analysis methods and tools effectively. Established exit criteria for each phase of analysis are useful.
- **Understand data flow and organization needs** associated with the analysis.

The Integrity of Analysis process tasks appear in Figure 4.9-4. Once the needs are understood clearly and addressed, the foundation is laid for managing the analysis set to obtain the needed results, which then serve as the basis to generate the AMP, as described in Integrated Technical Planning (Section 4.2).

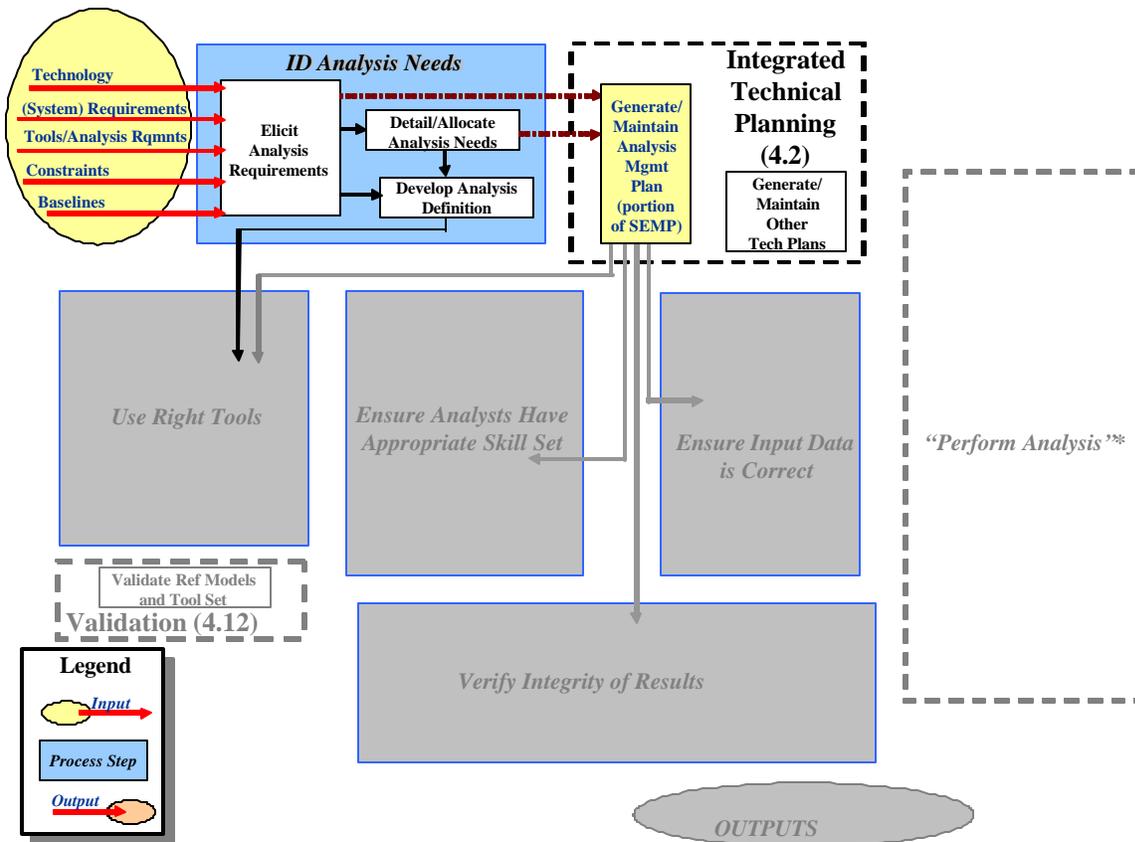


Figure 4.9-4. Identify Analysis Needs

Early analysis planning is key to program success. The quality of the analysis effort across the program is augmented by developing the program's AMP, a living document that manages and controls program analysis activities. The plan typically begins with a clear statement of project management goals, philosophies, and policies, followed by data to support planning for the analyses to be performed. The analysis needs are frequently a balance between the desires and costs of analytic excellence (usually championed by the analysts) and the cost/risk/benefit constraints of the program's budgets, schedules, and goals.

The AMP identifies required levels of analysis and the data to perform an analysis; defines procedures for ensuring analyst competency; contains details on the subset of analysis methods and tools that may be used for a validated analysis; and defines the criteria to ensure integrity of the analysis results. The plan provides specific tailoring required by the project and is updated when a new tool is validated on the program or when a currently validated tool is updated to reflect a change in the product design and is subsequently revalidated. Because new methods and tools may be needed for product variants, and because multiple versions of a product may exist concurrently, the AMP may reference multiple validated versions of the same tool.

#### 4.9.3.2 Task 2: Ensure the Right Tools Are Used

Developing meaningful system performance and cost estimates, establishing the associated system performance and design requirements, and defining acceptable tolerances may be accomplished only if analyses and performance models/databases are well defined and controlled and demonstrate validity. In addition, it is essential that analysis tool/model changes, updates, and predicted performance variances are properly identified and tracked over time. Independent but related tools/models and simulations must also be validated by comparison with a single reference baseline to ensure consistency of results.

An excellent and frequently stated guideline for choosing a tool/model is to select one that provides the most visibility into the problem but has the least complexity. It is recommended that practical tools/models include only features that are necessary for exploring the interactions between the study, object system, and its environment. There are many inhibitors to applying this guideline. Familiarity with a tool or a model often biases use of the tool. Lack of familiarity, inadequate training, or a "not invented here" syndrome may cause analysts to avoid a tool. The customer may expressly require use of a particular simulation tool or model. Management may demand that a single model be used throughout the program's life. A sound SE approach to select the right tool may overcome a number of these inhibitors. To ensure proper selection of a tool, it is recommended that the requirements of the analysis be considered, including:

- Analysis objectives
- Required level of fidelity and accuracy
- Cost controls
- Schedule constraints
- Need for additional resources

Analysis needs are allocated to tool components. Allocation includes assessing the level of fidelity required for each study function. For example, one study may require high fidelity if thrust, fuel flow, and range are being assessed, but lower fidelity in surveillance target selection. Tools that satisfy the functions and allocated study requirements for the model may be selected from existing tools or modifications to existing tools, or new tools may be created (Identify Candidate Tools task; see Figure 4.9-5). Each tool shall be examined to verify its ability to meet the analysis needs of the project before it is selected for use. Existing tools may not provide the functionality needed for the analysis. Under these circumstances, the project is faced with modifying an available commercial-off-the-shelf product, developing a proprietary tool for that application, or reconsidering the analysis scope. This evaluation shall be performed periodically to ensure that the tools continue to satisfy current project requirements. In addition, analysis shall be performed to assess the availability of new technology in tools, as it becomes available, and determine when it is prudent to switch to the newer technology, factoring in the costs of migration regarding people, time, and money. The considerations for selecting the right tool(s) appear in Figure 4.9-5 and discussed in detail below.

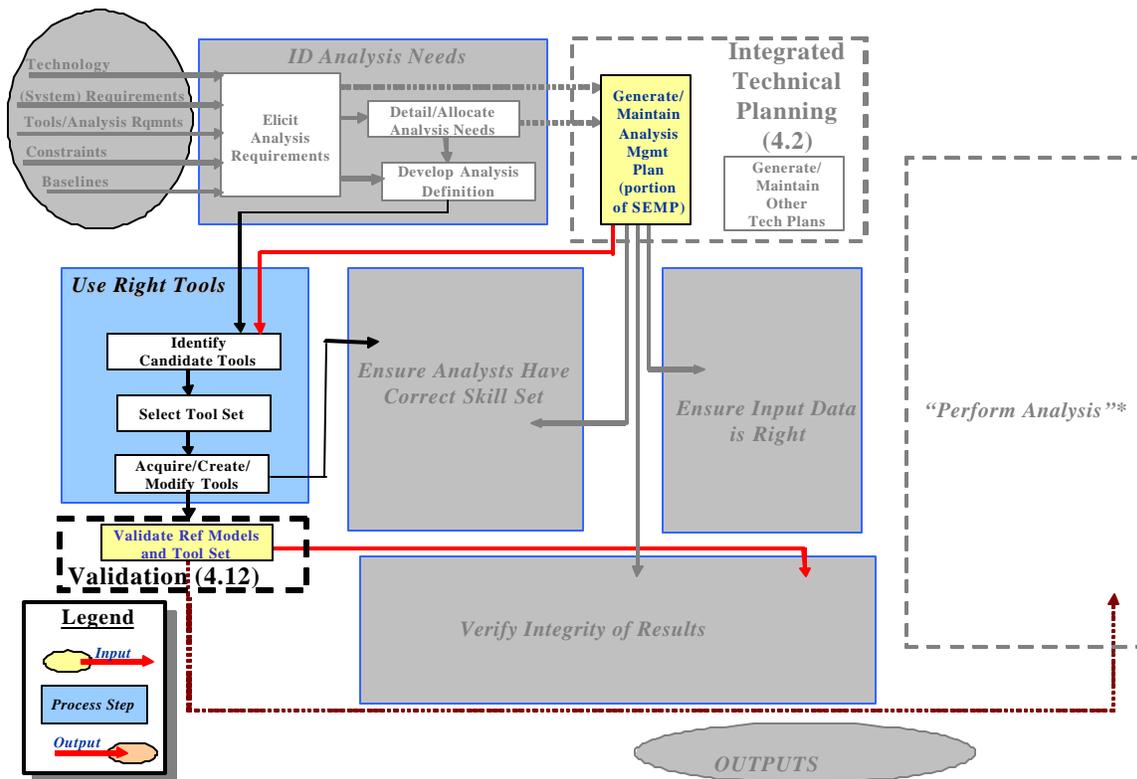


Figure 4.9-5. Use the Right Tools

#### 4.9.3.2.1 Tool Fidelity

One of the more misunderstood aspects of proper model selection is fidelity. High fidelity and high visibility into cause and effect are usually contradictory goals for a tool. As fidelity increases, basic top-level interactions and characteristics become obscured, which is particularly true of tools that incorporate random choices. Even in totally deterministic tools, the decision logic may become so complex that the visibility is lost. Occasionally, high fidelity may block goal achievement. High-fidelity tools often provide more than is realized, and analysts remain blissfully unaware of the true causes of model results.

For practical reasons, such as cost and schedule, the best choice is to use the least fidelity possible, but a model that still includes the desired effects. Interactions between system components and the environment that require modeling at a higher fidelity shall always be considered. If the system under study includes a human decision process, then one of the best ways to determine such interactions is by talking to people who operate the real system to determine what things they attempt to use to their advantage or what they attempt to avoid. A common belief is that all man-in-the-loop models are high fidelity and very complicated, which is not necessarily the case. In one example recently used by a military contractor, aircraft, ships, and missiles are point masses with movements constrained by very simple tables or equations. Sensor capabilities are modeled by simple equations that are one step above cookie cutters. Interactions with the environment, such as earth curvature and atmospheric attenuation on infrared sensors, are modeled equally simply. This example surfaced because of a deliberate attempt during requirements allocation on a specific project to emphasize human decision

making rather than hardware modeling. It is a good example of breaking the traditional mold with an inexpensive alternative that fully satisfies study needs.

At the other extreme, lack of fidelity may also distort answers. Operations analysts have used a series of air-to-air combat models to answer questions about such issues as the value of increased thrust in fighter aircraft. The early versions of these models used simplistic launch envelopes for the missiles with no provisions for infrared (IR) signature and missile-seeker effects. Head-on engagements with IR-guided missiles resulted in mutual kills. As a result, increased maximum thrust for close-in maneuvering combat on current generation aircraft like the F/A-18 or F-16 showed little improvement in expected kills and losses (two of the standard measures of effectiveness for combat aircraft). When moderately realistic IR features were introduced into the model, pilots were given the opportunity to reduce thrust in head-on situations and evaluate the results. Suddenly, the aircraft were spending about half of the engagement maneuvering in idle power to reduce the IR signature and increase survivability. Because there was much less time required to fly at maximum thrust to keep up aircraft energy (speed and altitude), the value of increased thrust over the shorter duration began to have a significant impact on the aircraft's effectiveness and survivability.

#### 4.9.3.2.2 Use of Validated Tools

Validation (Section 4.12) dictates that **any** error incurred in the examination or study is within a tolerance band that ensures that results satisfy the expressed need to the agreed confidence level. **A validated analysis method, model, or tool is defined as one that has been proven to provide credible results at the associated level of fidelity for a given analysis or study.** Validation may be performed using top-down or bottom-up techniques. Bottom-up validation is performed by comparing the methods and tool outputs, with varying sets of test case inputs, to the results of (1) another more complex validated model using the same test cases or (2) actual real-world performance (i.e., telemetry gathered in an actual flight). Bottom-up validation via real-world performance is usually difficult because it is nearly impossible to determine the model inputs required to simulate the real-world system. Top-down validation ensures credibility by verifying the top-down structure and performance of individual components. The best choice for validation is top-down because the issues are better understood, and there are fewer hidden assumptions.

For example, a software model that was previously validated to simulate an aircraft landing flight path without Global Positioning System (GPS) could be revalidated following the addition of a GPS receiver model in two ways:

- **Bottom-Up Validation.** The overall results of the entire model (with the new software for GPS added) are compared to either another model or real-world data.
- **Top-Down Validation.** Only the new software component added to simulate the GPS receiver (i.e., by comparison to actual hardware) and its interface with the other previously validated software are validated.

Regardless of whether it's a top-down or bottom-up validation, the algorithms and inputs used in the analysis tool shall be demonstrably correct and traceable back to their origin. It is a program management decision to determine the extent to use validated methods/tools. Examples of methods/tools that are candidates for formal validation include preflight modeling of unmanned aircraft/space vehicles, formal functional qualification testing, and Risk Management (Section 4.10). However, a significant amount of valuable analysis may be performed with unvalidated

tools. Use of an unvalidated methodology/tool simply introduces the additional risk that the results may have reduced credibility. Often, this risk is acceptable when weighed against the inconvenience, increased cost, or inability to meet a schedule that forces the analyst to use a validated method/tool. In most cases, a new or modified tool initially is used without validation, and a decision is made later regarding whether to perform validation based on expected future use of the tool.

#### 4.9.3.2.3 Tool Validation Process

Authorized analysis methods and tools are used over a broad spectrum of applications. Analysis tool validation is specific to the analyzed system(s) and performance for which the toolset is demonstrated. Both applicability and use are defined for every case validation. Situations may occur in which analysis data is required to support the program before full toolset validation. To address these situations, provisional and limited validations have been identified. Both types of validations exist to satisfy program needs for analysis data in advance of full validation; however, neither invalidates the need for full validation.

- **Full Tool Validation.** Tools are validated when they have met all accreditation requirements, have been recommended for validation by the responsible organization, and been reviewed by the Configuration Control Board (CCB) responsible for the baseline involved. (Configuration Management (Section 4.11) provides more information on this topic.)
- **Provisional Tool Validation.** Provisional validation may be granted when model performance has been essentially demonstrated, but compliance with all validation requirements has not been achieved.
- **Limited Tool Validation.** Tool validation may be limited to indicate that performance demonstration for full validation is incomplete, though all data indicate that model performance is correct and consistent for a limited analysis. Documentation requirements may be tailored for limited validation.

The analysis toolset validation process supports and is key to the analysis oversight responsibilities of each implementing program. Validation is based on demonstrating model performance, analyzing toolset configuration management/controls, and documenting the analysis methodology. As part of the approval process, the program manager designates approval authority for formal validation, which may be accomplished by forming an Analysis Review Board or through the Program CCB, as discussed in Configuration Management (Section 4.11). This designation is typically reflected in the AMP or Analysis Management section of the SEMP. If an Analysis Review Board is established, its membership may consist of program management, a member of SE, and a member of each project team using the analysis tools. The Program Board (Analysis Review Board or CCB) reviews applicability and use for which the analysis tool suite is to be validated. The term "CCB" is used for this board throughout the rest of this section.

Once the analysis method/toolset has been authorized for use, the implementing program determines whether the toolset requires validation for its usage and the degree of validation. The degree of validation required varies with the lifecycle stage and other factors. Methods of validation include verifying the ability of the tool to provide answers for known test cases or to crosscheck the results with other tools or methods for agreement.

The tool validation portion of the AMP specifies what is to be tested, how it is to be tested, and what comparisons are to be made to the relevant reference check cases and other data in validating the analysis methods and tools. Reference check cases give the responsible organization a comparative way to demonstrate that a toolset may be validated. It is recommended that comparison of analysis data to reference check case data be included as the first step in any validation plan. To complete validation, the responsible organization may propose any cost-effective combination of the following methodologies listed in order of decreasing priority:

- Comparison of data with the real system
- Comparison to other analysis applications whose validation basis is actual test comparison
- Comparison of data with other validated toolsets
- Technical audit of toolset performance
- Demonstration of toolset capability

It is recommended that a sensitivity analysis be performed to characterize the behavior as each input is individually varied. The purpose for which the toolset is being validated is the primary concern in determining the mix of methodologies selected for validation.

**Demonstrated performance is defined as the ability of an analysis to produce results that compare favorably with results obtained from the system being modeled over common areas of performance.** The responsible organization proposes its performance demonstration as part of the AMP. The overall demonstration shall be controlled by a matrix that has analysis capabilities/characteristics on one axis and test scenarios (demonstrations) on the other axis. This matrix identifies how each analysis capability/characteristic is to be demonstrated for the purpose of certification. Once all performance demonstrations have been completed and action items assigned to the responsible organization(s) are closed, the CCB reviews the toolset validation package for completeness and assesses the need for further review before approving the validation package. In addition, this validation test matrix provides the CCB a guide to validation requirements and completion status, and is developed by the responsible organization. This matrix is provided as part of the validation plan and is used by the CCB at subsequent review meetings to track validation completion status.

#### 4.9.3.2.3.1 Validation Approval Package

The final validation package shall conform to the approved AMP. Approval of the following documentation is required as part of the Analysis toolset validation process:

- AMP
- Configuration Control Plan sections related to analysis toolset control
- Analysis certification report
- Analysis tool users manual
- Analysis tool version definition

A member of the responsible organization presents the validation package to the CCB for final approval. Once the package has been approved, the CCB provides the responsible organization a signed validation certificate.

#### **4.9.3.2.4 Validated Methods and Tool Configuration Management**

The responsible organization maintains Configuration Management (Section 4.11) and controls the validated set of tools. All validated methods and tools are under configuration control and are documented in the approved Program Analysis Management and Configuration Management plans. Validated tool Configuration Management shall ensure traceability of all changes to validated tools over time, identification of the specific versions of the toolset used to develop analysis results, and the specific configuration of embedded hardware/software subsystems or components being modeled.

##### **4.9.3.2.4.1 Criteria for Analytical Tool Validation Update**

Changes within the analysis toolset that do not introduce changes to modeled systems or their performance domain do not require a validation update as long as regression testing demonstrates identical results. The responsible CCB defines specific validation update requirements for each analysis toolset as part of the review. The following guidelines are used to determine if a validation update is required:

- If the analysis tool revision creates significant differences in analysis results, applicability, or use
- If there is significant program visibility and community interest in a functional characteristic that was modified
- If there are significant hardware/component changes to the systems being addressed that impact reference models, databases, or simulations
- If change accumulations account for a significant deviation from the previously validated baseline

If required changes impact more than one tool or model, the responsible CCB must ensure that all affected tools/models are appropriately revised and that changes installed continue to provide comparable analysis results to the standard reference set of baselines. In every case, the responsible CCB may reassess the applicability to determine if the changes are required.

#### **4.9.3.2.5 Analysis Reference Standards System**

Analysis results are not expected to precisely replicate results from the modeled system(s). Additionally, analysis results may not be consistent among themselves. Analyses are compared to a standard reference set of baselines to ensure consistency of results when they are used to substantiate and evaluate specific areas of system performance. Only reference analyses, reference models, and reference databases are employed as performance or design baselines.

##### **4.9.3.2.5.1 Reference Analyses**

A set of authorized, validated analyses (certified in the case of simulations) is established as reference analysis methods. Accreditation of reference methods usually includes validation using actual test data. Reference simulations serve as the principal performance baseline(s) for the appropriate CCB action and provide a point of departure for derived analyses that may be

used to establish the effect of proposed system design changes or to assess system sensitivities. Reference analysis methods typically include reference models and/or databases and are used to generate reference check cases.

#### **4.9.3.2.5.2 Reference Models**

In cases where overlap exists between elements being modeled by more than one validated tool, the function modeled in one particular validated tool is identified by the CCB as a standard for comparison, or reference model. Reference models are established to capitalize on primary expertise in specific areas of performance and to provide consistency at the subsystem level. Reference models shall be segregated, validated, and made available to the analysis community.

#### **4.9.3.2.5.3 Reference Databases**

A reference database is one that represents the selected subsystem performance through tabulated values. Reference databases are established in cases where there is no advantage to modeling a subsystem function. Reference databases are created by a model that is used to generate tables of values that constitute the database. The database then represents the selected subsystem performance through tabulated values. Reference databases are established by the responsible CCB to provide consistency at the subsystem level, take maximum advantage of specific areas of expertise, and simplify analyses.

#### **4.9.3.2.5.4 Reference Check Cases**

Reference check cases are a representative set of conditions or characteristics for a situation under study that is used as the basis for certification comparison. Reference check cases are selected, reviewed, and distributed to each CCB and are available to the responsible organizations as the basis for certification comparison. Reference check cases are generated by reference analysis methods, often are based on actual test events, and include relevant inputs, initial conditions, assumptions, and expected outputs in a form (e.g., hardcopy and/or electronic media) usable by each responsible organization for subsequent analyses.

### **4.9.3.3 Task 3: Ensure Analysts Have Appropriate Skill Set**

The previous subsections on using the right tools addressed the level of confidence required for each analysis, as stated in the AMP. Part of that confidence, from a programmatic sense, is derived from the proficiency of the analyst. Quantification of that component of confidence may be difficult or impossible to precisely determine, but qualitatively it needs to be addressed. Three elements are involved: (1) establish the training required, (2) select the analyst(s), and

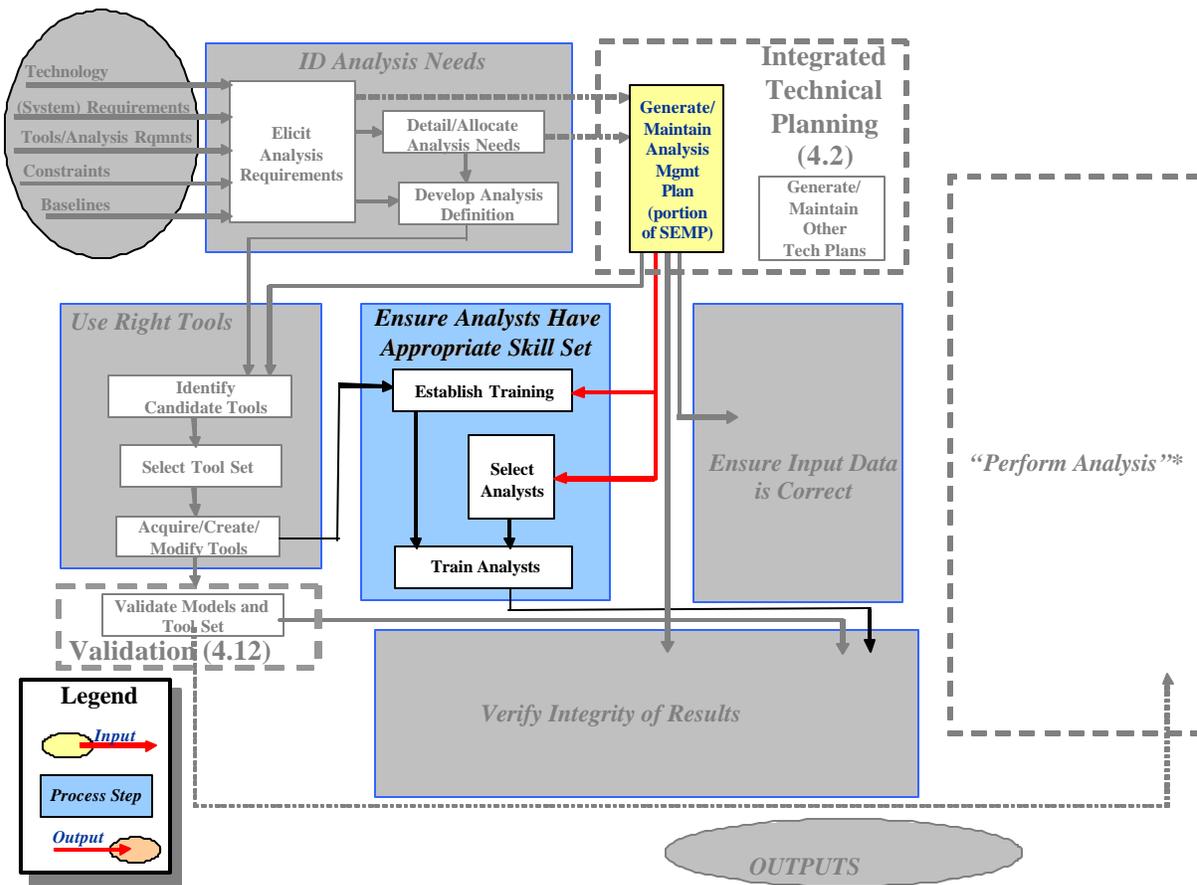


Figure 4.9-6. Ensure Analysts Have Appropriate Skill Set

(3) train the analyst(s) based on a gap analysis between the skill set required to perform the analysis and the skills the analyst already possesses.

The AMP shall describe the approach to be used for each type of analysis to ensure that the analyst possesses the necessary level of proficiency to perform that type of analysis, including level of difficulty. Such approaches include:

- Acceptance of credentials (e.g., validated professional degrees, personnel performance reviews, known track record) or stipulation by supervisors. The currency of such information is important—this aspect is addressed in the “Establish Training” element (see Figure 4.9-6).
- Training accomplished within a defined previous period (and whether subsequent test or demonstration of performance validated such training). In the sense of on-the-job training, a policy of ongoing revalidation of analysts is useful, if for no other reason than to maintain a current roster of analysts and their credentials.
- Satisfactory performance in a validation trial to be judged against prescribed target results.

An extreme case, in which the program may be at great risk unless a particular analysis has a very high confidence, may lead to the need to: (1) certify analysts as world-class experts in using a particular version of the tool to be used; (2) ensure that the experts have recent experience in its use in a very similar application; and (3) require a number of identical but independent analyses by different but independent analysts to produce results within a specified tolerance of each other, or against a reference case or test data. An example would be the thermal analyses that were required early in the International Space Station program that were necessitated by a proposed change in orbit inclination coupled with a major change in assembly sequence in orbit.

For the purposes of this manual, programmatic issues as well as purely technical issues are included. Consequently, it is appropriate to discuss the distinction between competence and proficiency. Competence deals with one's ability to achieve excellence in results, no matter how much it takes. Analysts may be distinguished on the basis of the ease, speed, and/or clarity with which they produce results. No guidelines are offered herein, but it is recommended that the matter be addressed in the AMP.

Another evaluation method is the technique of peer review. The practice of using a nearby colleague (typically of approximately the same competence) to review the analysis has been shown to be useful. In analytic work, the opportunities for simple neglect or even typographical errors are great, and it is impossible to easily detect personal errors; however, with peer review, these kinds of problems are more easily found. An analyst may believe he/she is capable of a certain job (and credentials may imply that), but peers may discover that his/her sphere of expertise does not include the analysis in question. (The most dangerous situation is often when the analyst does not realize what he/she does not know.) The AMP documents the implementation of program management's policies in this area. This process task appears in Figure 4.9-6 above.

#### **4.9.3.4 Task 4: Ensure Input Data Is Correct**

It is ultimately an analyst's responsibility to determine that the data used in an analysis is appropriate for that analysis. This responsibility then flows upward in a program and organization, and the AMP addresses how that member's responsibility shall be supported. Special attention should be paid to instances where analyses need to be merged or where one analysis provides input data for use in subsequent analyses. In such cases, it is especially necessary for analysts to use compatible data that agree in quality and type. The considerations involved appear in Figure 4.9-7.

##### **4.9.3.4.1 Data Sources and Control**

The AMP specifies acceptable sources for each type of data: general or universal data (such as atmospheric properties); corporate data (possibly proprietary, such as material properties or design limits); and program-specific data (tradeoff factors such as the partial derivative of aircraft range regarding takeoff weight for a nominal mission). Organizational standards and libraries may exist that may be referenced, and a program may supplement those with program-unique data or even define its own.

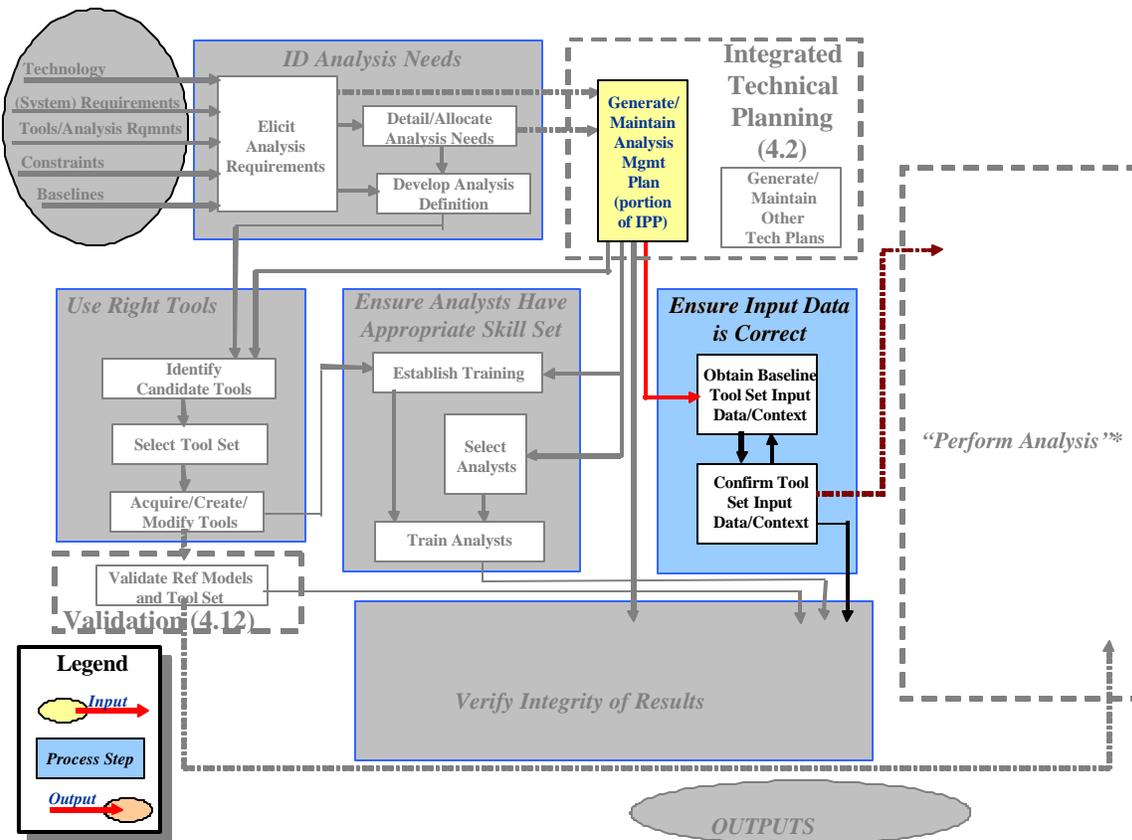


Figure 4.9-7. Ensure Input Data Is Correct

The object is to provide baselined data and configuration control of that baseline by the process defined in the program plan. Using baselined data results in traceable analytic results. The consistency derived from all analysts using the same baselined data produces results that may be confidently merged, compared, and/or interpreted. Besides the issue of where the data physically resides and from where it may be retrieved, there is the need to document and control the identification of the data's original source. If it represents measured data, its measurement error, range of uncertainty, or confidence interval shall be recorded.

#### 4.9.3.4.2 Data Quality

One factor that shall be determined for each planned analysis is the **numerical confidence interval** that is acceptable in the results, which, in turn leads to a requirement for precision, accuracy, and granularity of the input data, as well as its treatment within the algorithms. Note that granularity includes the effect of decisions regarding the number of significant digits to be used. (There is no difference between declaring Pi to be 3.14 and defining it as the ratio of a circle's circumference to its diameter if both are measured to 3 significant digits.) Where the scope, required level of precision, or coarseness of an analysis calls for it, the AMP shall specify how baselined data may be approximated or "granulized."

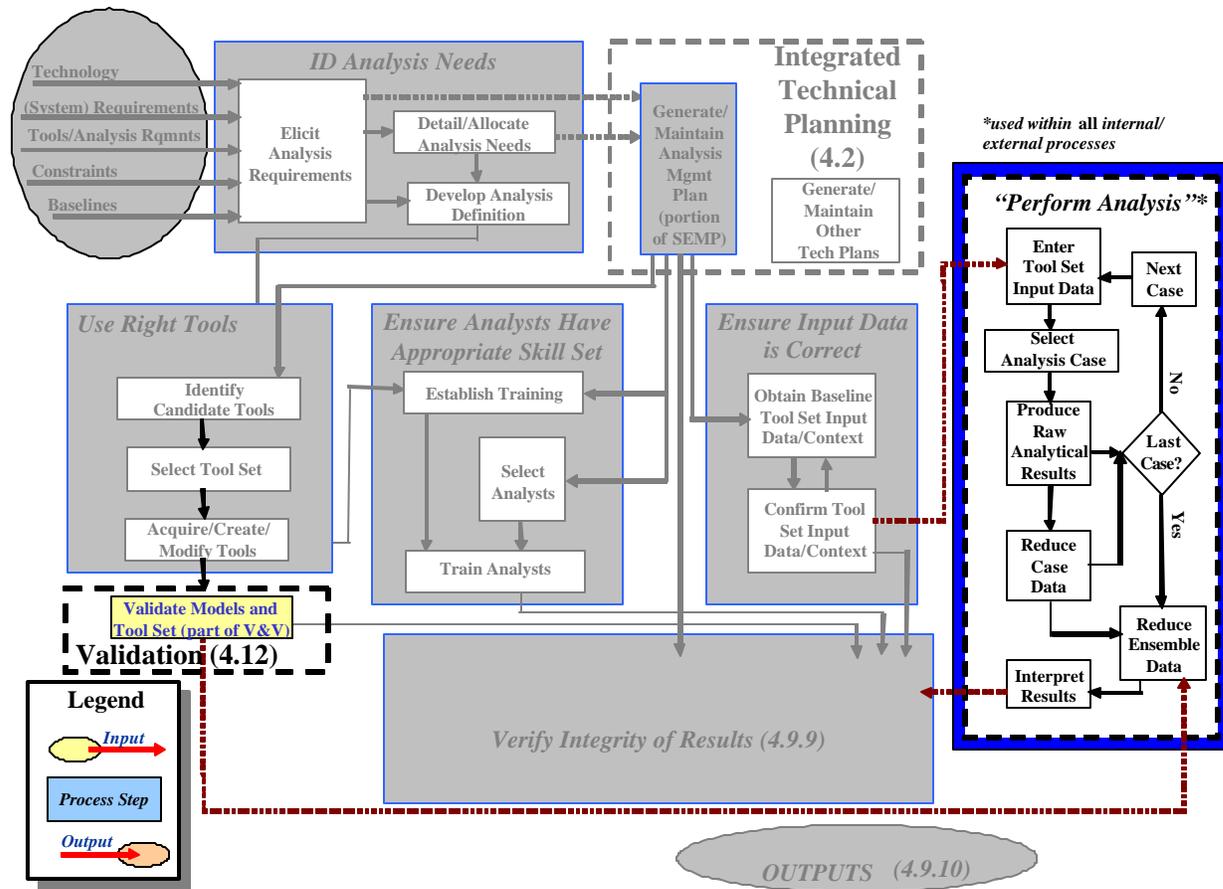


Figure 4.9-8. Perform Analysis (Reference)

#### 4.9.3.4.3 Documentation of Data Within Analyses

An analysis is ultimately credible if it can be independently repeated. When repeatability is considered, it is clear that part of that ability is knowing exactly what data was used to create the first result; therefore, that data shall be carefully documented. The source, pedigree of validation, and extent of accuracy, precision, and granularity shall be documented. Thus, the reader will have the confidence that **all** the data were considered, even constants and parameters that are frequently forgotten, especially if they may have been “hard-coded” within a relation or equation.

#### 4.9.3.5 Task 5: Perform Analysis (Reference Task)

The other sections of this manual describe the actual analyses performed. The Integrity of Analysis process supports the other SE processes and is intended to provide a disciplined framework for conducting any required analysis, whether technical, programmatic, or administrative in nature. The interaction between the Integrity of Analyses process and the actual performance of analyses appears in Figure 4.9-8.

### 4.9.3.6 Task 6: Verify Integrity of Results

In general, an analysis is useless unless it may be independently repeated; therefore, the inputs and all underlying assumptions shall be documented (Figure 4.9-9). It is recommended that criteria be established in the AMP for each type of analysis to ensure that the results are accurate, correct, and sufficient. The criteria are enforced by developing, validating, and using analysis templates. Comparing results from two or more truly independent analyses may be performed to achieve confidence in the results when the accuracy and/or validity of the analysis tools and methods have not been proven. It has been shown repeatedly that the greater the independence of the individual analyses, the greater the confidence the stakeholders have in the validity of the result.

Sufficiency of the analysis shall also be addressed: Did the analysis consider the entire envelope of interest? Were the selected portions of the envelope adequate to draw a proper conclusion? Did the analysis account for all significant effects? In rare cases, it may be necessary to perform additional analysis to determine precisely which effects need to be considered to substantiate the results of an analysis.

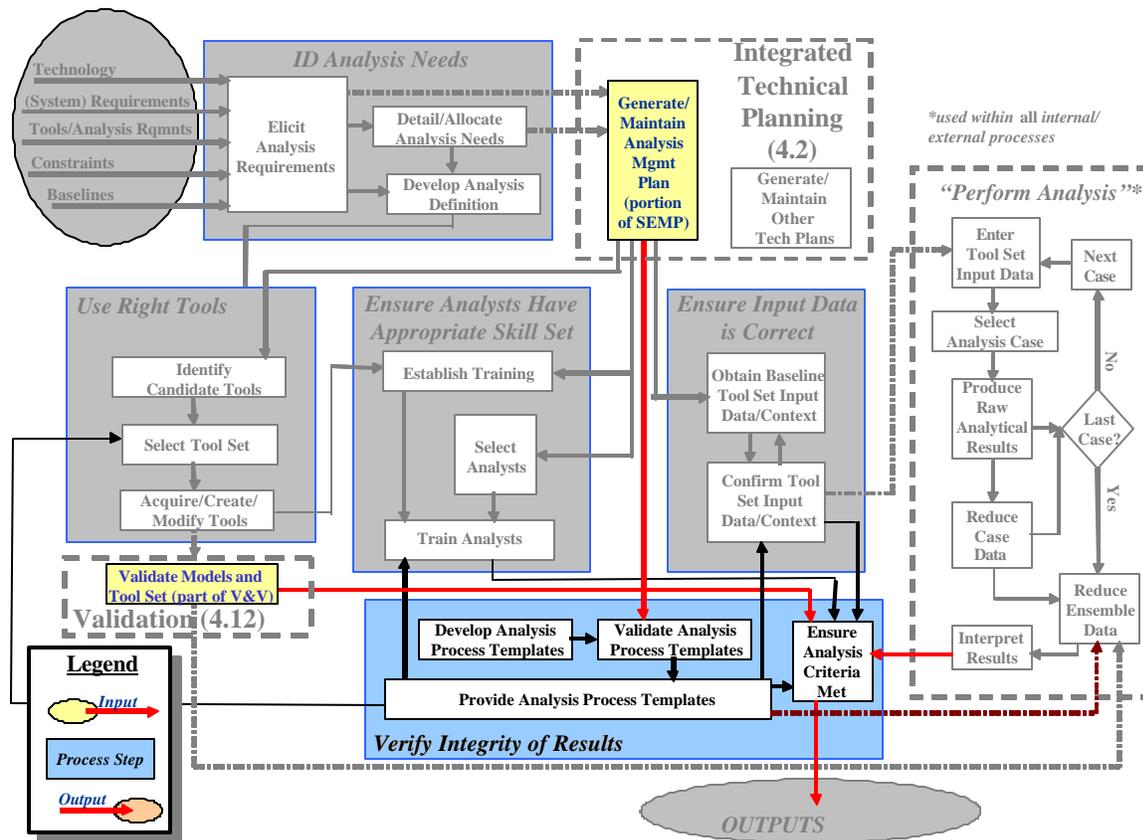


Figure 4.9-9. Verify Integrity of Results



- Even though a modeling technique or simulation tool has been proven to be completely accurate, errors may still be present in an analysis. Such errors may be caused by omitting terms that have a significant effect on the result, using the wrong input data (e.g., wrong atmospheric model), and misinterpreting or misunderstanding input data (e.g., wrong units or wrong reference coordinate system). Independent analysis may catch these errors only if there is no collaboration between the analysts. The criticality of the results of the analysis should determine the degree of verification justified.
- Another type of innocent error is caused by an analyst's misunderstanding of the problem statement (i.e., requirements). In this case, a completely valid answer may be presented to the wrong question.
- An analysis may be nothing more than an opinion poll. Evaluating the characteristics of the population considered only ensures this accuracy of this type of analysis.
- Ultimately, the results are verified by users per the original plan. If the results are insufficient, then a root cause analysis is performed where appropriate. The outcome of this analysis may result in the original analysis being reconducted by modifying:
  - Methods
  - Tools
  - Inputs
  - Users

#### 4.9.4 Outputs of Integrity of Analyses

The two major outputs of this process are analysis criteria captured in the AMP, which includes the appropriate tools and/or reference models, and credible analysis results (Figure 4.9-10). In addition, any residual concerns and issues generated by this process are furnished to the Risk Management process (Section 4.10) for resolution. Any constraints driven by tool selection, skill requirements, or other programmatic considerations documented in the AMP are furnished to the Requirements (Section 4.3) and Trade Studies process (Section 4.6) to assist in defining the appropriate trade space. Planning criteria is furnished to the Integrated Technical Planning process (Section 4.2) for planning purposes. Training conducted under the auspices of the Maintain Process element (Section 4.14) uses material from this section.

##### 4.9.4.1 Analysis Criteria

The degree of validation required for each tool and type of analysis shall be specified. Tools as

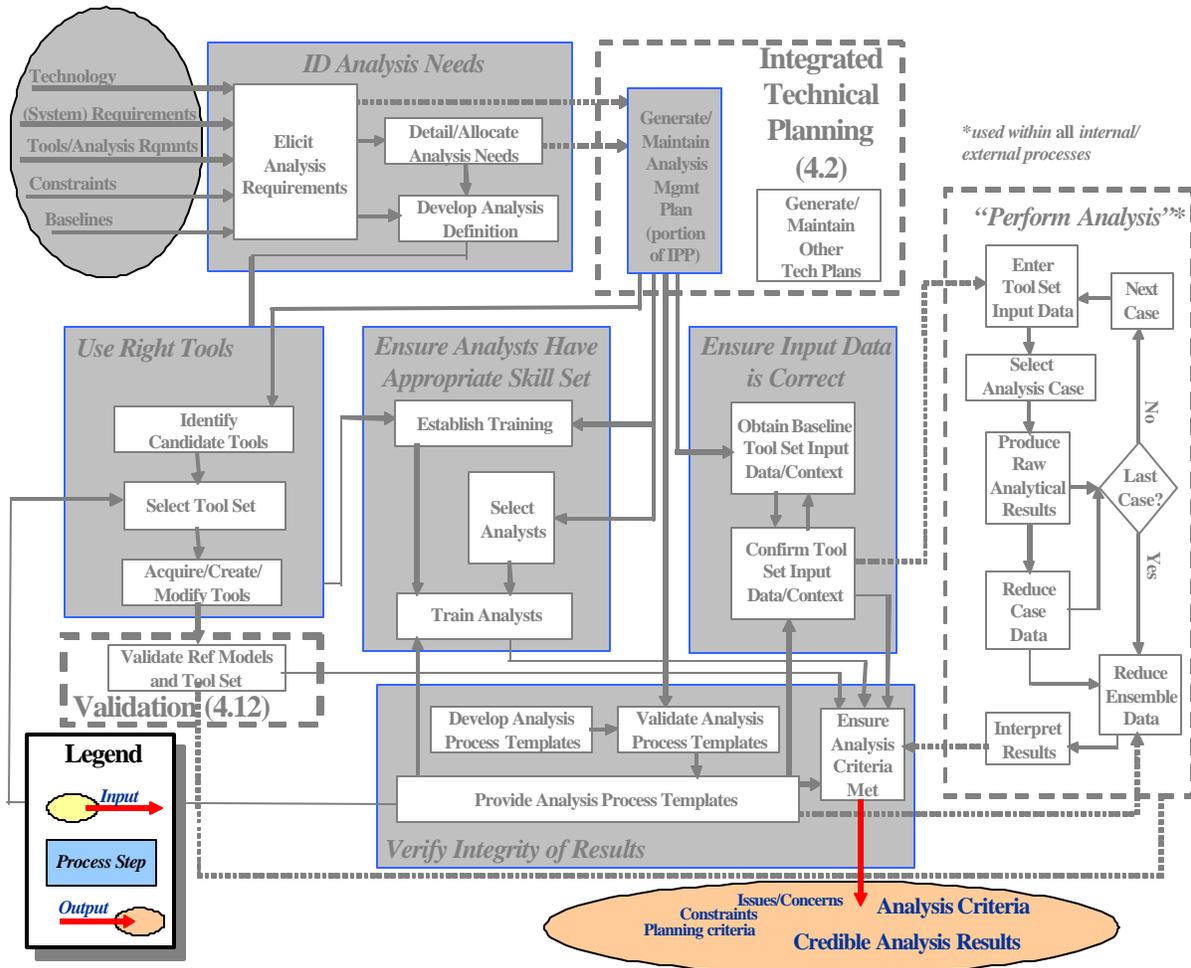


Figure 4.9-10. Integrity of Analyses Outputs

simple as an Excel spreadsheet or as complex as man-in-the loop simulations may be used to support programmatic decisions. A method shall be developed to verify that the correct equations are used for the analysis and that they have been properly implemented in the spreadsheet. Whatever the tool, the plan specifies the procedure for acquiring/developing, maintaining, and validating that tool. Typically, a program has a configuration control function (its own or some core organization's) from which validated tool lists may be drawn and referenced.

The AMP is also used to specify the analysis methodology to be imposed. It is recommended that every analysis be understood as being bounded or constrained by all the pressures implied above. It is important to capture these issues in the AMP so that aspects such as the following are treated in the plan.

- Methods shall be specified to ensure that analysts are proficient in using the tools and executing the analyses. This consists of providing proper documentation, training, and review procedures.

- Methods and analysis criteria shall be specified to ensure that data of the proper quality and range, from documented sources with valid pedigrees, are under configuration control and, thus, traceable when referenced by the analysis documentation.
- The required level of documentation for each type of analysis shall be specified, usually in the form of templates. Formal analysis shall provide sufficient documentation to permit reconstruction of the results from the input data. Quick analysis used to rule out a possible system design may not require the level of documentation or substantiation as analyses that are required to support the final system configuration.
- The review policy for each type of analysis shall be specified.

#### 4.9.4.2 Credible Analysis Results

Simulated results are not expected to precisely replicate results from the simulated systems. Additionally, analysis results may not be consistent among themselves. Models shall be compared to standard reference baselines to ensure consistency of results when employed to substantiate and evaluate specific areas of system performance. Only reference simulations, reference models, and reference databases may be employed as performance or design baselines. Analysis results are meaningless without description of the analysis method and the assumptions that generated those results. If the tool version used to generate the results is not validated, the differences between the validated version and the version used, as well as the validation plans for the new version, are also to be presented.

#### 4.9.5 Integrity of Analyses Process Metrics

Table 4.9.1 shows the four general measurement categories that apply to Integrity of Analyses along with candidate measures for analysis management. It is recommended that each effort tailor these measures and add other project-specific measures that are applicable to ensure that they contribute the necessary information to the decision-making processes.

**Table 4.9-1. Integrity of Analyses Measurement Categories**

Schedule and Progress	Resources and Cost	Product Quality	Process Performance
Percent of analysis tasks completed on schedule	Existing validated model is ratio of analysis to total hours  ( <b>Total</b> = analysis hours + verification hours)	Percent of analysis "passing" verification step (first pass)	Average number of days to complete analysis (per same tool and complexity)

## 4.10 Risk Management (*Satisfies iCMM Process Area (PA) 13 criteria*)

### 4.10.1 Introduction

The objective of Risk Management is to provide a proper balance between risk and opportunity. It seeks to understand and avoid the potential cost, schedule, and performance/technical risks to a project, and to take a proactive and well-planned role in anticipating them and responding to them if they occur. Risk Management is equally at home in project management as well as System Engineering (SE) because both domains have a common view of seeking out opportunities to solve a problem or fulfill a need. Opportunity represents the potential for improving value in achieving a goal; risk represents the potential for decreasing the same value. Hence, any discussion of Risk Management is concomitant with the subject of opportunity management. The methodologies, decision parameters, and outcomes apply as well to risks as they do to opportunities.

The Risk Management process (Figure 4.10-1) provides an organized, systematic decision-making methodology to effectively deal with uncertainty in accomplishing program and/or organizational objectives. **Risk is defined as 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.**



The PMBOK® Guide Chapter 11 Project Risk Management states that risks can have a positive or negative outcome. The approach outlined in this chapter recognizes risk as dealing with the negative side of the value proposition and recognizes that the positive side of the value chain is reserved to the management of opportunity.

**Risk Management is an organized, systematic decision-support process that identifies risks, assesses or analyzes risks, and effectively mitigates or eliminates risks to achieve objectives.** A risk creates an exposure to failure based on the combined effect of its likelihood and consequence, referred to as the “risk exposure”. Because the risk exposure 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. This means that the process is applied to small projects and large programs, across all aspects of a program or organization (see Figure 4.10-2), and continuously throughout the program's lifecycle. The extent and depth of application of this process should be governed by the outcome(s) being supported. In other words, what decisions are involved at a given point in the lifecycle, and what are the relevant risk factors to be addressed to support those decisions? The risks shall be managed in a way that they are capable of being “rolled up” from a project or several projects to a program. Risk rollup involves a review of the consequences/impacts from a higher (program or organizational) level. The risks to meeting the objectives or benefits of these projects or programs are typically known as programmatic risks, though the source of these risks may be external to the program itself. This process complies with the requirements of the integrated Capability Maturity Model (iCMM) (PA 13). It also satisfies Electronic Industries Alliance (EIA) 632 requirement 24 and EIA 731 Focus Areas 2.5-2 through 2.5-8.

For the purpose of this section, the terms “program,” “project,” and “organization” are used interchangeably, except where the context infers otherwise. In those instances, a program is generally viewed as consisting of related projects and is usually part of an organization.

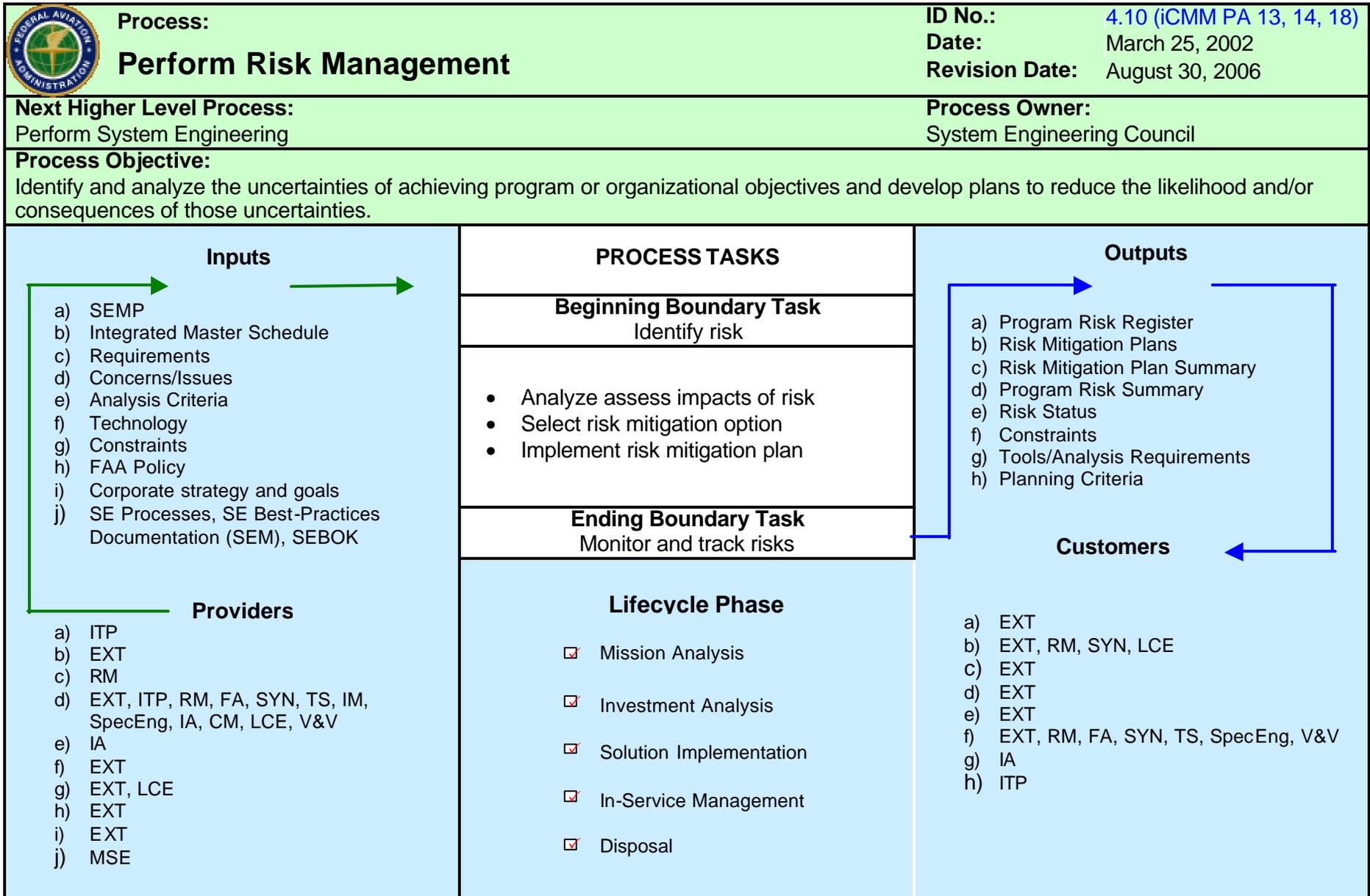
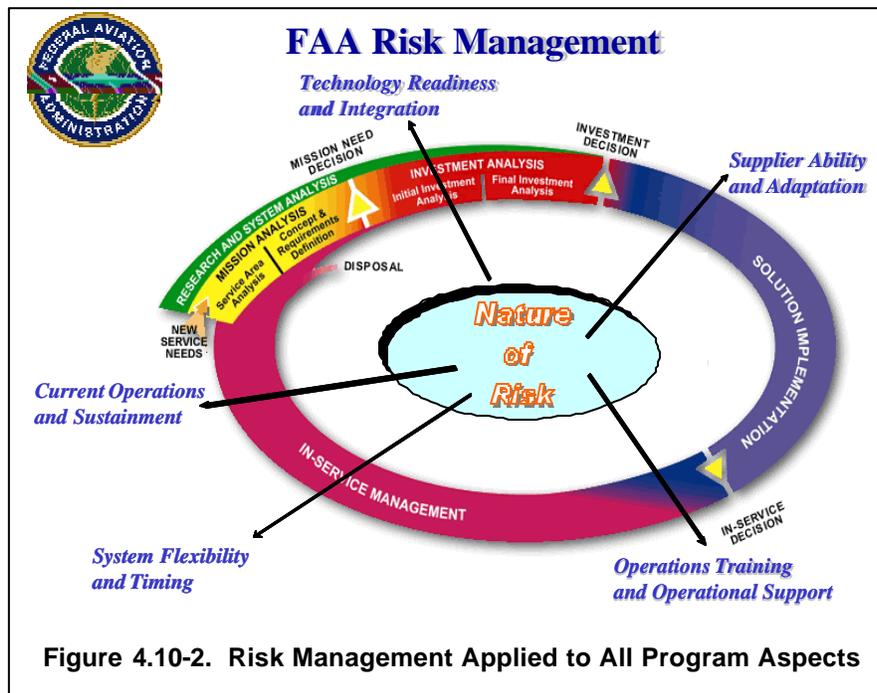


Figure 4.10-1. Risk Management Process-Based Management Chart



#### 4.10.1.1 Function of Risk Management

Risk management is a basic SE element of successful program management (Figure 4.10-3). When properly executed, Risk Management engages all disciplines and execution teams and is present in all program stages and phases. The functions (Figure 4.10-4) of the process are to:

- Identify each risk to the program
- Analyze and assess the negative consequences/impact and the likelihood/probability of the risk actually occurring and determine the risk realization date
- Develop specific approaches and plans to mitigate the risk
- Implement the risk mitigation plan
- Monitor and track risk mitigation effectiveness

Based on results from these functions, program management may then determine:

- The schedule and budget reserves to be allocated and to what, based on identified risks
- 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

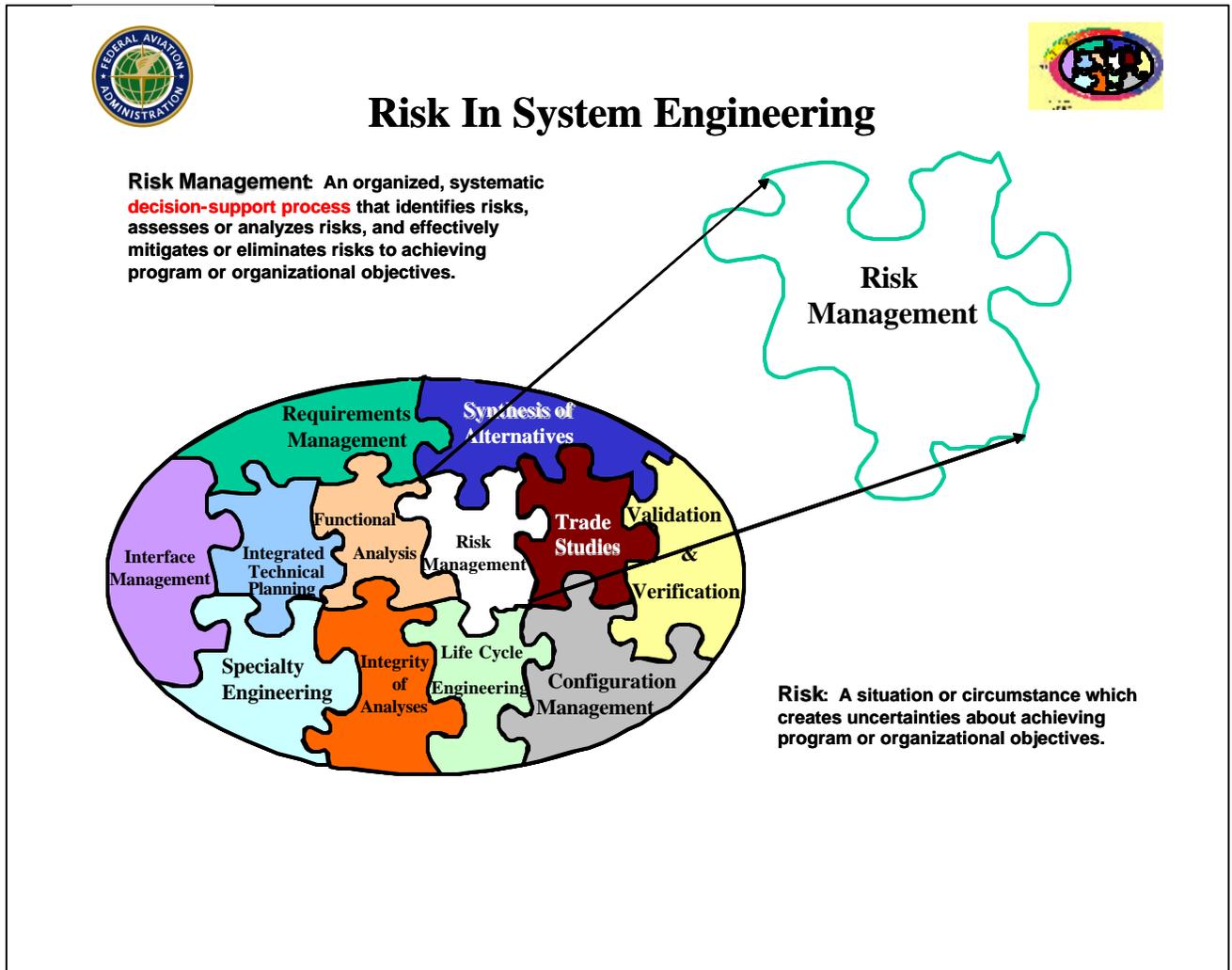


Figure 4.10-3. Risk in System Engineering

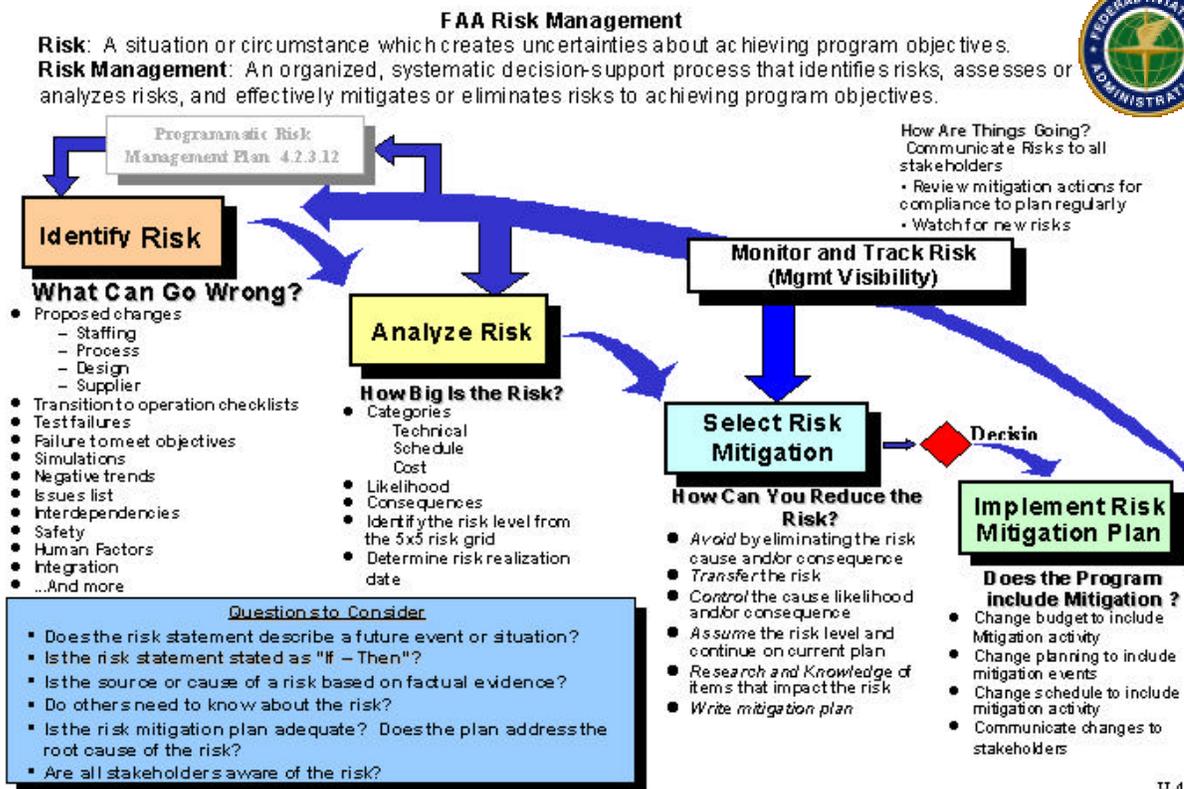


Figure 4.10-4. FAA Risk Management Process

#### 4.10.1.2 Objectives of Risk Management

Within the opportunity-risk paradigm, the fundamental objective of the Risk Management process is to identify and analyze uncertainties of achieving program or organizational objectives and develop plans to reduce the likelihood and/or consequences of those uncertainties.

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 risks (identifying a potential problem with sufficient lead time so that the team may implement appropriate alternate plans)
- Consistent assessment of the level of risk across a program (providing a structured decision making framework for prioritizing resource application)
- Communication of risk mitigation actions across the program/organization (ensuring that all elements of the program/organization are aligned in resolving risks)
- Review of risk mitigation action performance

#### 4.10.2 Process Description (*Satisfies iCMM PA-14, BP13.04 criteria*)

Every participant in a program/organization shares the responsibility of assessing and mitigating risks. The process is a part of the overall program/project management and system engineering process(es). This process shall be aligned with the individual products (hardware, services, and

software) that result from consistent functional analysis and requirements allocations, the System Engineering Management Plan (SEMP), the integrated program schedule, the associated funding, and the identified goals and benefits. The effort involved is assessed as to risks associated with impacts on benefits, interdependencies with other programs/organizations, or environments. For each product, risks are evaluated against the established operating baseline technical requirements, schedule, and cost leading to the successful satisfaction of the program/organizational objectives. Risks are identified, assessed, and appropriate risk mitigation actions established that comply with the governing risk management plan (see Section 4.2, Integrated Technical Planning). This plan is developed and tailored (when the nature of the effort demands tailoring per Section 3.5) to satisfy the specific program/organizational needs. *(Satisfies iCMM BP 13.01 criteria)*

Results from each assessment are a starting point for the risk mitigation plan to support management decisions (technical, schedule, and cost). The products of this process are also shared with stakeholders to achieve alignment/acceptance of the resource decisions. All risks are examined at each program/project/event/item/peer review as defined in the risk management plan. Updates reflect changes in risk resulting from planned mitigation activities or other unplanned events. Risk progress is actively tracked. For each risk, a “risk realization date” is established, marking the point in time when either the risk no longer exists or when the risk becomes a fact, and the program may have to be modified to accommodate the negative consequences. This point in time can be expressed as either an absolute (date, etc.) or in relative terms (project milestones, events, etc.). The question to be asked and answered is: “What happens at this point in time?” Risk is “rolled up” when it is taken from a lower-level project to a higher-level program or from a lower-level organization to a higher one for review and mitigation.

An essential element of the Federal Aviation Administration (FAA) Risk Management process from an organizational point of view is the non-advocate concept. The purpose of a non-advocate is to provide an impartial, objective assessment of the project team's results, especially regarding assignment of risk levels. The input of a non-advocate is essential on those projects where two or more of the project specialists disagree on the risk levels. A non-advocate would typically be, but not limited to, a program management person (above or at the same level of the program/project manager); a stakeholder representative; and/or a person from another project or program. The responsibility of a non-advocate is to examine and assess all aspects of the program/project risk management process before each review. For small projects, one or two non-advocates may be acceptable. A non-advocate provides an assessment to program/project managers for consideration and action.

#### **4.10.2.1 Overview**

Figure 4.10-1 shows the top-level process for Risk Management. The 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 Plan, and monitoring of risk status. The process is iterative and is used across the program throughout the program's lifecycle, with the nature of the risks changing to coincide with the lifecycle stage. Table 4.10-1 illustrates the

Table 4.10-1. Risk Management and the AMS Lifecycle Phases

Risk Activity	R&D to Mission Analysis	Initial Investment Analysis	Final Investment Analysis	Beyond Investment Analysis
Risk Focus	Assessment of operational risk associated with new concepts	Assessment of comparative risks between alternatives	Lifecycle risks of the selected alternative; Risk Management Plan updated for Implementation	Program execution Acquisition and/or Program Reviews
Depth of Risk Assessment	High-level	Some detail	More detailed	Detailed
Risk Products	Identification of potential risks  General risks and requirements for any proposed alternative	Comparative risk analysis for each alternative  Initial risk-adjusted cost and benefits baseline	Updated Risk Analysis  Risk Management Plan (in SEMP)  Final risk-adjusted cost and benefits Baseline	Risk Management Plan  Risk Tracking Matrix  Etc.
Risk Leadership Role	Stakeholder/Organization	Investment Analysis Team	Investment Analysis Team	Program/Sponsor/ System Operator

lifecycle dimension of Risk Management. Specific knowledge domains implement variants of this process to fit their specific needs and environment. However, all domains effectively perform Risk Management, as shown in Figure 4.10-4.

#### 4.10.2.2 Inputs

An expanded set of inputs capable of initiating Risk Management includes both program/project and product-related data as shown in Table 4.10-2. Many of these inputs are developed and refined through the continuous, iterative use of other system engineering processes. Each table item is to be evaluated for resultant program risk. (Items in bold appear in Figure 4.10-1 Process-Based Management Chart.)

Table 4.10-2. Inputs to Risk Management

Input	Reference
<b>Risk Mgmt Plan</b>	4.2.1
System Engineering Management Plan (SEMP)	4.2.3.2
Integrated Safety Plan	4.2
Implementation Strategy and Planning	4.2
Test plans	4.12
<b>Integrated Program Schedule</b>	4.2
<b>Requirements</b>	4.3.3
Mission Need and Concepts	4.4
Interfaces	4.7
Statement of Work	4.3
<b>Issues/Concerns</b>	Appendix D
Trade Study Results	4.6.1.4
Design Analysis Results	4.8.4.3
Controlled Data and Reports	4.11.8
Specialty Engineering Analysis Results	4.8
Safety and/or Security Assessments	4.8
Human Factors Assessments	4.8
Verification Results	4.12
Training Results	4.14
Maintenance Results	4.13
Operational Results	4.13
Lessons Learned	4.14
Program Review Results	4.2.6
<b>Analysis Criteria</b>	4.9.5.5
<b>External Environmental Forces</b>	
ISAP (Internal Exhibit 300)	FAST
System Engineering Reviews	4.2.6
Contractor Outputs	
<b>Technology</b>	
<b>Constraints</b>	
Enterprise Architecture (EA)	4.5.5
Manufacturing/Production Information	4.5
Product Configuration Data	4.11.3
Resources/Budgets	
<b>FAA Policy</b>	
AMS Documents	FAST
<b>Corporate Strategy and Goals</b>	
Contract	

### 4.10.3 Risk Management Process Tasks

Figure 4.10-1 summarizes the Risk Management process. The remainder of this section describes the major process steps, as shown in Figure 4.10-4.

#### 4.10.3.1 Task 1: Identify Risk (*Satisfies iCMM BP 13.02 criteria*)

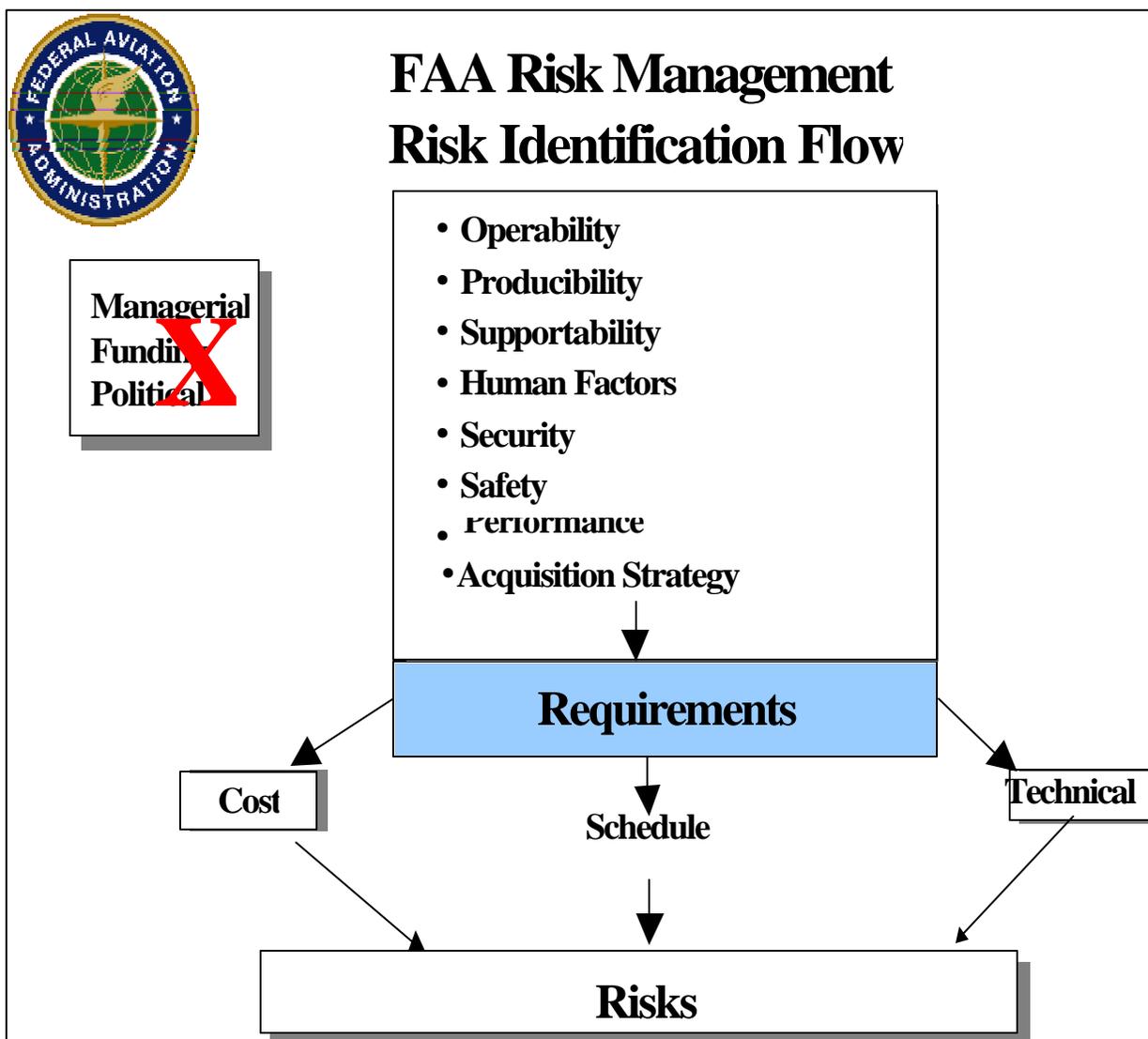
**Risk identification is a systematic effort to uncover possible events or conditions that, if they occur, may hinder achievement of program or organization objectives.** The process begins concurrently with program or project planning and continues throughout the life of the program. In each instance, the question to be asked is: "What can go wrong or interfere with success?" While risk events or conditions may have many different root causes (e.g., equipment interoperability requirements, maintainability and supportability requirements, installation deadlines, contractual arrangements), the identification process isolates those events or conditions that may affect program technical performance, cost performance, or the program schedule. At the conclusion of the identification phase of risk management, it is recommended that a program manager have a list of (uncertain) events and conditions that may affect program cost, schedule, and/or technical performance. Risk identification shall be performed during each stage of the program, or whenever significant changes occur in plans or program status. Circumstances requiring assessment for potential risks 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
- Special assessments at the direction of agency management
- Changes or risks in interdependent programs
- Environment changes

As shown in Figure 4.10-5, 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.



A risk has three aspects: (1) the event is in the future, (2) the likelihood/probability that an event will occur (a degree of uncertainty), and (3) a negative or unfavorable consequence/impact if it occurs. It is recommended that the likelihood of a risk occurring not be



**Figure 4.10-5. Risk Identification Flow**

so low as to be negligible (i.e., probability essentially equal to zero) nor be equal to 1, which typically indicates that it has, in fact, already been realized. A risk shall also have a negative consequence/impact if realized. If ANY of these three characteristics are missing, the situation under consideration is handled as either an issue or a concern.

Positive variances to plan or consequences are not considered in the FAA risk identification and analysis process; these are considered opportunities. Note that if **ANY** of these three aspects are missing (i.e., the situation or circumstance is certain to occur or has already occurred), there is no risk, even though the item has an unfavorable consequence. It is recommended that this situation be handled as a management issue or concern, for which a corrective action plan shall be generated and implemented.

As discussed in subsection 4.10.2 above, each risk has a “risk realization date”. The negative consequence of the outcome of the event that occurs on a given date is the basis for the risk. It is very important to identify and document this point in time as early as possible to ensure that only active risks consume the organization’s attention and resources.

#### 4.10.3.1.1 Potential Sources of Risk

Risks originate 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. Figure 4.10-5 shows a risk identification flow. 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/program, and *funding* is the supply of money provided to accomplish a given project/program. The risk source is based on the **root cause** of the risk and, as such, only a single source will cause a risk. The source is either technical, schedule, or cost in nature and not a combination or all of these. This is not to be confused with the symptoms, which may manifest themselves as some combination of performance (technical), benefit, cost, and/or schedule impact.

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 commercial-off-the-shelf (COTS) solutions. Risks that need to be considered in a COTS-based acquisition appear in Figure 4-10.6.

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, additional complexity, change in economic conditions, competitive environment, supplier viability, and lack of applicable historical data.



Table 4.10-3 provides the potential sources of risk that shall be considered in the process of program risk assessment. This listing provides an excellent starting point for identifying potential risk areas when combined with the input factors appearing in Table 4.10-1, Risk Management and the AMS Lifecycle Phases.

**Table 4.10-3. Potential Sources of Risk**

<b>Program Aspect</b>	<b>Common Risk Areas</b>
<b>Architecture</b>	<ul style="list-style-type: none"><li>• System requirements flow-down not well defined.</li><li>• Trade-off studies not performed early enough in the program to support system design with the best alternative.</li><li>• Modeling and simulation use limited in more fully developing and evaluating potential architectures.</li><li>• Functional interfaces between architecture elements not well defined.</li></ul>
<b>Capability of Developer</b>	<ul style="list-style-type: none"><li>• Developer has limited experience in specific type of development.</li><li>• Contractor has poor track record relative to costs and schedule.</li><li>• Contractor experiences loss of key personnel.</li><li>• Contractor has poor track record relative to appropriate training for personnel.</li><li>• Prime contractor relies excessively on subcontractors for major development</li></ul>
<b>Concurrency</b>	<ul style="list-style-type: none"><li>• Immature or unproven technologies will not be adequately developed before production.</li><li>• Production funding will be available too early, before development effort has sufficiently matured.</li></ul>
<b>Contracting</b>	<ul style="list-style-type: none"><li>• Acquisition strategy unstable or changing; untimely acquisition strategy approval.</li><li>• Key program documentation (specifications, interface documents) unavailable to support RFP package release.</li><li>• Overall program definition (program strategy) unclear; cannot be clearly defined in program Statement of Objectives (SOO) for definition to the contractor.</li><li>• Request for Proposal (RFP) package release schedule does not support overall program schedule needs.</li><li>• Realistic cost objectives not established early.</li><li>• Marginal technical capabilities incorporated at excessive costs.</li></ul>
<b>Cost/Funding</b>	<ul style="list-style-type: none"><li>• Satisfactory cost- technical tradeoffs not done.</li><li>• Excessive life cycle costs due to inadequate treatment of support requirements.</li><li>• Significant reliance on software.</li></ul>

**Program  
Aspect**

**Common Risk Areas**

- Design implications not sufficiently considered prior to investment decision.
- System will not satisfy user requirements.
- Design**
  - Mismatch of user manpower or skill profiles with system design solution or human-machine interface problems.
  - Increased skills or more training requirements identified late in the acquisition process.
  - Design not cost effective.
  - Design relies on immature technologies or “exotic” materials to achieve technical objectives.
- Integration**
  - Interface documentation is inadequate or not defined.
  - End to end performance has not been addressed.
  - System integration with legacy configurations is unclear.
- Lifecycle**
  - Inadequate supportability late in development or after fielding, resulting in need for engineering changes, increased costs, and/or schedule delays.
  - Lifecycle costs not accurate because of poor logistics supportability analyses.
  - Logistics analyses results not included in cost-performance tradeoffs.
- Management**
  - Acquisition strategy does not give adequate consideration to various essential elements (as mission need, operations, test and evaluation, technology).
  - Subordinate strategies and plans are not developed in a timely manner or based on the acquisition strategy.
  - Proper mix (experience, skills, stability) of people not assigned
  - Effective risk assessments not performed or results not understood and acted
- Production/  
Facilities**
  - Production implications not considered prior to investment decision.
  - Production not sufficiently considered during design.
  - Inadequate planning for long lead items and vendor support.
  - Production processes not proven.
  - Prime contractors do not have adequate plans for managing subcontractors.
  - Operational requirements not properly established or vaguely stated.
  - Requirements are not stable.
- Requirement  
Set**
  - Required operating environment not described.
  - Requirements do not address logistics and suitability.
  - Requirements are too constrictive—identify specific solutions that force high cost.
  - Requirements are not verifiable.

<b>Program Aspect</b>	<b>Common Risk Areas</b>
<b>Safety</b>	<ul style="list-style-type: none"><li>• Safety management program not established early in the life cycle.</li><li>• Program and subject matter expert coordination is limited with safety professionals.</li><li>• Safety analysis assumptions inadequate or not defined.</li><li>• Safety analyses not performed on changes.</li></ul>
<b>Schedule</b>	<ul style="list-style-type: none"><li>• Schedule not considered in trade-off studies.</li><li>• Schedule does not reflect realistic acquisition planning.</li><li>• Schedule objectives not realistic and attainable.</li><li>• Resources not available to meet schedule.</li><li>• System security requirements not specified sufficiently or timely enough to support system design needs.</li></ul>
<b>Security</b>	<ul style="list-style-type: none"><li>• System security interface definition (cryptography, keys, fill devices, message structure) with the individual program elements is unclear or immature.</li><li>• Limited program involvement and coordination with system security developers and providers (NSA for example).</li><li>• Security implications not adequately considered in architecture.</li><li>• Uncertainty in threat accuracy.</li><li>• Tools and reference models are not validated.</li></ul>
<b>Simulation</b>	<ul style="list-style-type: none"><li>• Maintenance and Support are not verified, validated, or accredited for the intended purpose.</li><li>• Program lacks proper tools and modeling and simulation capability to assess</li><li>• Program depends on unproved technology for success—there are no alternatives.</li></ul>
<b>Technology</b>	<ul style="list-style-type: none"><li>• Program success depends on achieving advances in state-of-the-art technology.</li><li>• Potential advances in technology will result in less than optimal cost-effective system or make system components obsolete.</li><li>• Technology has not been demonstrated in required operating environment.</li></ul>
<b>Test and Evaluation</b>	<ul style="list-style-type: none"><li>• Test planning is not initiated early in program.</li><li>• Testing does not address the ultimate operating environment.</li><li>• Test procedures do not address all major technical and suitability requirements.</li><li>• Test facilities not available to accomplish specific tests, especially system-level tests.</li><li>• Insufficient time allowed in the schedule to test thoroughly.</li></ul>

## COTS Considerations

<i>Number</i>	<i>COTS Risk Factor (Characteristic)</i>
<b>01</b>	<b>COTS products can exhibit rapid and asynchronous changes.</b>
<b>02</b>	<b>COTS product obsolescence can affect systems in different ways.</b>
<b>03</b>	<b>COTS products are typically documented with proprietary data.</b>
<b>04</b>	<b>Low initial costs of COTS products can be offset by higher lifecycle costs.</b>
<b>05</b>	<b>Functionally equivalent COTS products/systems can have multiple configurations.</b>
<b>06</b>	<b>Different COTS product vendors have different quality practices.</b>
<b>07</b>	<b>COTS products form, fit, and function are sold “as is.”</b>
<b>08</b>	<b>COTS products are developed to commercial standards.</b>
<b>09</b>	<b>COTS products typically have time-limited manufacturer support.</b>
<b>10</b>	<b>COTS product interoperability can introduce information security susceptibility.</b>

**Figure 4.10-6. COTS-Based Risk Considerations**

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 vulnerability to cause harm. The combination of a viable threat coupled with a 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.

### **4.10.3.1.2 Risk Identification Methods**

Risk identification begins at the lowest feasible level and normally includes inputs from all stakeholders and suppliers. Anyone may identify a potential risk. The objective of this step is to produce a list of potential risks that is as comprehensive as possible. It is recommended that the focus be on root causes and not on symptoms of a more basic problem. The problem shall be defined at the lowest level (root cause) so that the mitigation plan actually addresses the problem. It is recommended that experts review previous programs to determine that risks related to their domain(s) have been completely identified. It is also recommended that similar programs be reviewed for determined risks as well as actual problems. This may be achieved using any combination of methods, such as group discussions, interviews, trend/failure analysis, risk templates, lessons learned, trade studies, best practices, metrics, and acquisition documentation.

This process includes a final step to validate or screen the list of proposed risks prior to committing them to the risk repository or database. This validation should ensure that the risks identified are germane to the effort at hand and look for duplication and consolidation as appropriate. A “risk owner” should be assigned to each validated risk in accordance with the provisions of the Risk Management Plan (RMP) to manage the efforts associated with and be responsible for that risk as it progresses through its own lifecycle. Once the proposed risk has been entered into the organization’s master risk database, it has effectively been approved by management as warranting further effort to address. The extent of that effort is governed by the provisions of the RMP.

Program Management errors are not risks and shall be corrected before the program moves forward. It is recommended that this screening consider program-level ramifications and ensure that program integration risks are adequately covered.



A Risk Worksheet (Figure 4.10-7) may be used to document newly identified potential risks and provide a documented trail of actions taken to determine the plan to reduce a given risk to an acceptable level.

#### 4.10.3.1.3 Risk Statements

Risk statements frame the problem space. The investment made in properly structuring the risk statement is inversely proportional to the effort expended to deal with the risk. If little to no effort is expended upfront, then a disproportionate amount can be spent “chasing” the wrong problem. A rule of thumb for identifying risks is to state each risk candidate in “condition ... if ... then ...” format. If a certain event occurs, then there will be a certain consequence. Using this form makes it is easy to determine the validity of a risk. This construct generates a “strong” risk statement.

If the statement does not make sense or cannot be put in this format, then the candidate is probably not a true risk, and the resulting statement is considered weak. For example, a statement that has the “if” element but not the “then” implies that the potential event will not affect the project. Similarly, a statement with the “then” element but not the “if” implies there is an issue that will certainly affect the project, but no uncertainty about its occurrence. Table 4.10-4 contains some examples of weak risk statements gleaned from recent FAA Exhibit 300s prepared for submittal to the Office of Management and Budget (OMB). Each example has one or more essential elements missing to define the problem space and provide a solid basis for actions taken to deal with the (perceived) risk.

**Table 4.10-4. Weak Risk Statements**

If COTS components become technically obsolete before planned, the system could be difficult to maintain, maintenance costs could rise, or tech refresh could be required sooner than planned.
(Deployed) systems could become inoperative due to hardware and or COTS obsolescence.
Investment fails to deliver promised capability to field sites due to failure to take holistic view of effort.
Instability in the market place may lead to a supplier being unable to continue (to participate) in (this program).
Internal and external risks for (the system) gathering weather data and processing it into usable

and accurate weather information. <i>(Note: This is reviewed on an Annual basis. July 2004)</i>
(There may be) sudden or critical reductions in key project resources that can hinder the normal (project) processes. <i>(Note: This is reviewed on a weekly basis. 02/15/05)</i>
Technology (being used) not adequate for future requirements and expansion.
The government does not have experienced personnel for the management and acquisition of this investment.



A strong risk statement includes descriptions of the future event or condition, which confirms a potential problem; the root cause(s) of the event outcome or conditions; and the specific negative consequences to the program if the event or conditions occur. Subsection 4.10.3.2.3 discusses the methodology to determine the relative import of a risk. The construct of a strong risk statement provides a powerful means to accomplish that task. Table 4.10-5 illustrates the characteristics of strong a risk statement extracted from examples in recent FAA Exhibit 300s prepared for submittal to OMB (details have been changed for illustrative purposes).

**Table 4.10-5. The Anatomy of a Strong Risk Statement**

(Risk #216) <b>If</b> either the multiple SMR SAT completion or the start of the ASDE-X Safety Logic Optimization by July 15, 2006 is delayed in any way, <b>then</b> the commissioning of the new Atlanta ATCT and the IOC date of May 1, 2007 will be delayed, which will not meet the terms of the AT/NATCA MOU.
(Risk #305) <b>If</b> the Safety logic design and associated performance does not meet the operational expectations at Orlando International (MCO), <b>then</b> the ability to achieve ISD and deploy at other sites per the deployment schedule will be at risk with continued potential of accidents caused by runway incursion incidents at those locations.
(Risk # 389) <b>If</b> adjustments are not made to the installation schedule to accommodate aggressive intervals for key activities, the ASDE-X system may be in jeopardy to meet the Operational Required Date at Seattle International ... in time to support the decommissioning of ASDE-3 in August 2007, as required in the MOU with the Port of Seattle.

**4.10.3.2 Task 2: Analyze and Assess Impacts of Risk (Satisfies iCMM BP 13.03 criteria)**

Risk analysis or risk assessment provides program insight into the significance of identified risks. Risk analysis attempts to assess the likelihood of identified risks and the consequence to the program/organization if the risk event or condition occurs. The process also classifies each risk according to the root cause of the risk event (cost, schedule, or technical performance).



### FAA Risk Worksheet

Program/Project Title \_\_\_\_\_ Seq. #: \_\_\_\_\_

Submitted by: \_\_\_\_\_ Date: \_\_\_\_\_

Risk:	Point of Contact
-------	------------------

Source and Root Cause:

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th colspan="3" style="text-align: left;">Risk Assessment</th> <th style="text-align: left;">Rationale</th> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/> Technical</td> <td style="padding: 2px;"><input type="checkbox"/> Schedule</td> <td style="padding: 2px;"><input type="checkbox"/> Cost</td> <td></td> </tr> <tr> <td style="padding: 2px;">Likelihood</td> <td colspan="2" style="padding: 2px;">A B C D E</td> <td></td> </tr> <tr> <td style="padding: 2px;">Consequence</td> <td colspan="2" style="padding: 2px;">1 2 3 4 5</td> <td></td> </tr> </table>	Risk Assessment			Rationale	<input type="checkbox"/> Technical	<input type="checkbox"/> Schedule	<input type="checkbox"/> Cost		Likelihood	A B C D E			Consequence	1 2 3 4 5			
Risk Assessment			Rationale														
<input type="checkbox"/> Technical	<input type="checkbox"/> Schedule	<input type="checkbox"/> Cost															
Likelihood	A B C D E																
Consequence	1 2 3 4 5																

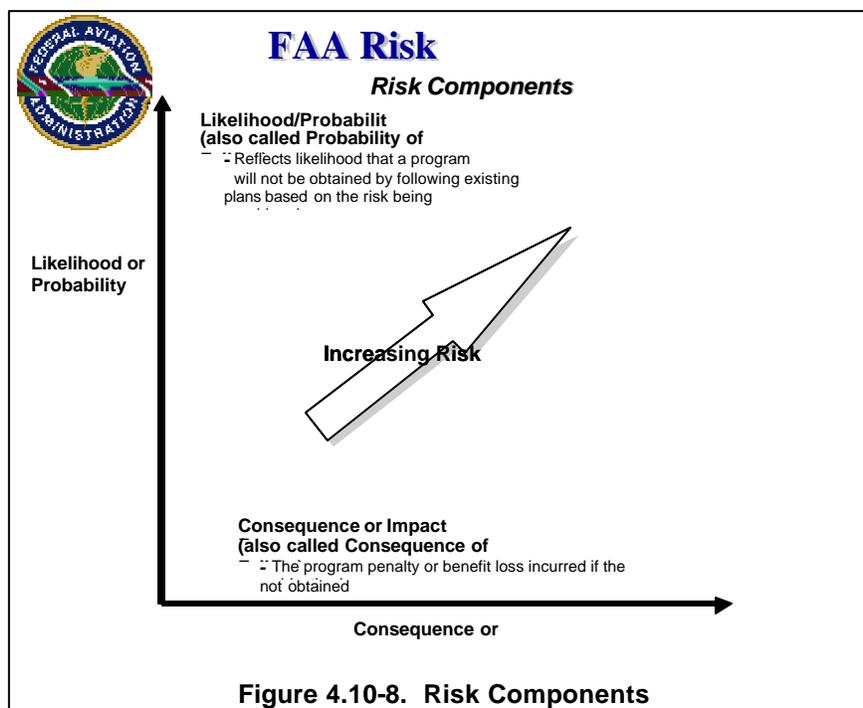
<p style="font-size: small;">             Likelihood              E              D              C              B              A              1 2 3 4 5              Consequence              High              Medium              Low         </p>	Consequence Definition:
---	-------------------------

Risk Realization Date: \_\_\_\_\_

5	Mitigation Options	Description	New Risk Level if Implemented
<input type="checkbox"/>	Avoidance		H M L
<input type="checkbox"/>	Transfer		H M L
<input type="checkbox"/>	Control		H M L
<input type="checkbox"/>	Assumption		H M L
<input type="checkbox"/>	Research & Knowledge		H M L

Submitted: _____	Date: _____	<input type="checkbox"/> Mitigation Approved	<input type="checkbox"/> Disapproved
Approval: _____	Date: _____	<input type="checkbox"/> Approved w/ Change	<input type="checkbox"/> Returned
		<input type="checkbox"/> Risk Accepted	<input type="checkbox"/> Closed

Figure 4.10-7. Risk Worksheet



Risk analysis assesses each of the two components of an identified risk — (1) the likelihood of the risk occurring, and (2) the consequence to the program if it occurs — as depicted in Figure 4.10-8. The basic tool used for qualitative risk analysis is the risk template, which contains a set of definitions to be used to evaluate the likelihood and consequence of a particular risk. The set of templates that a program uses may change over time as new templates are added or existing templates are changed, combined, or eliminated. The program may choose to use program-unique templates, which are based on and traceable to program or stakeholder requirements, provided supporting rationale is given. However, modification of templates limits the ability to “roll up” risks to a higher program level, and, as such, a mechanism shall be developed to correlate risks developed through modified templates to the risks developed with the standard FAA templates. The program/project is responsible for the choice, coordination, and control of the templates used on the program. These decisions are contained in the Risk Management planning section of the SEMP (see Section 4.2, Integrated Technical Planning of this document).

The result of the risk analysis process is assignment of a measure termed “risk exposure” to each identified risk. Risk exposure is one quantitative figure of merit that represents the combined effects of likelihood and consequence; it aids program management in ranking identified risks from most severe to least severe. At the conclusion of the risk analysis process, it is recommended that program management have visibility into the range of possible outcomes for the program (in terms of achieving objectives) if in fact an identified risk event or condition occurs.

#### 4.10.3.2.1 Likelihood (Probability) Determination

A likelihood (probability) template is developed that applies to the specific risk/program under analysis. A new template is developed and documented if none of the existing program templates are applicable. This action shall be coordinated within the program/project and with higher levels of the organization using the criteria of the RMP. Correlation of the new templates

to the standard FAA templates in this manual shall be established. Figure 4.10-9 provides the FAA definitions of the risk likelihood levels.

#### **4.10.3.2.2 Consequence Determinations**

Another set of templates is used to evaluate consequence/impact to the program if the risk materializes. Consequences are ideally expressed in terms of dollars, specifically the cost of loss or recovery from that loss. Because of the difficulty of determining the costs in advance, templates are used to categorize the risks into relative groups of impact. Consequence templates are shown for three areas of program impact: technical (Figure 4.10-10), schedule (Figure 4.10-11), and cost (Figure 4.10-12). The choice of the consequence template to be used to evaluate a given risk is determined by the nature of the root cause of that risk. If the root cause is technical in nature, then the technical consequences template is used. It should be remembered that each of these templates results in a risk that threatens the benefits of a program and may also have interdependency impacts. The symptoms of the risk may materialize in any combination of program areas: technical (or performance), schedule, and/or cost. However, treating only the symptoms wastes program resources and does **NOT** directly deal with the source or root cause of the risk.

All NAS programs are developed to provide benefit(s) to the system. Risk ultimately reflects in impacts to benefit(s). All benefit losses are derived from negative impacts in either technical, schedule, or cost risks. This is a significant part of the risk consequence that must be defined. The cost/benefit analysis should be reexamined as a result of risk-driven impacts to provide the information needed to make informed decisions. As was the case with the likelihood templates, if none of the existing program consequence templates are applicable to a particular risk, new templates may be developed and documented. Correlation of the new templates to the standard FAA templates in this manual shall be established.



## FAA Risk Likelihood Definitions

*What is the likelihood the risk will happen?*

- A. **Not Likely:** Your approach and processes will effectively avoid or mitigate this risk based on standard practices (<10% chance it **WILL** occur).

*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 processes to be well understood and documented. Little or no management oversight will be required.*

- B. **Low:** Your approach and processes have usually mitigated this type of risk with minimal oversight in similar cases (<1/3 chance that it **WILL** occur).

*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.*

- C. **Likely:** Your approach and processes may mitigate this risk, but workarounds will be required (~50% chance that it **WILL** happen).

*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.*

- D. **Highly Likely:** Your approach and processes cannot mitigate this risk, but a different approach might (>2/3 chance that it **WILL** happen).

*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.*

- E. **Nearly Certain:** Your approach and processes cannot mitigate this type of risk; no known processes or workarounds are available (>90% chance that it **WILL** happen).

*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.*

**Figure 4.10-9. Risk Likelihood Definitions**



## FAA Technical Consequence Definitions

*Given the risk becomes real, what would be the magnitude of the impact on system performance?*

1. **Low:** Given that the risk is realized, there would be minimal impact.  
*A successful outcome is not dependent on this issue; the technical performance goals will be met. There would be no impact on the success of the program.*
2. **Minor:** Given that the risk is realized, there would be a minor performance shortfall but the same approach could be retained.  
*The resulting technical performance would be below the goal but within acceptable limits. There would be no need to change the basic design, process, or approach. There would be no impact on the success of the program.*
3. **Moderate:** Given that the risk is realized, there would be a moderate performance shortfall but workarounds would be available.  
*The resulting technical performance would be below the goal. The basic design, process, or approach could be retained with only minor changes, and the overall system performance would still be acceptable as a result of workarounds such as the reallocation of functions or performance goals. There would be only a limited impact on the success of the program.*
4. **Significant:** Given that the risk is realized, the performance would be unacceptable but workarounds would be available.  
*The resulting technical performance would be unacceptably below the goal. The design, process, or approach would require a significant change to achieve an acceptable performance level. Additional workarounds such as the reallocation of functions or performance goals could also be required. The success of the program could be jeopardized.*
5. **High:** Given that the risk is realized, the performance would be unacceptable with no known workarounds.  
*The resulting technical performance would be unacceptably below the goal. There are no known alternatives or solutions. The success of the program would be in doubt.*

Figure 4.10-10. Technical Consequence Definitions



## FAA Schedule Consequence Definitions

*Given the risk becomes real, what would be the magnitude of the impact on the schedule?*

1. **Low:** Given that the risk is realized, there would be minimal impact.  
*The program schedule is not dependent on this issue. There would be no impact on the success of the program.*
2. **Minor:** Given that the risk is realized, additional activities would be required to meet key dates.  
*One or more key dates in the program schedule, but not critical path events, would be jeopardized; there are identified schedule workarounds that would be sufficient to mitigate the schedule impact. There would be no impact on the success of the program.*
3. **Moderate:** Given that the risk is realized, there would be a minor schedule slip, and one or more need dates would be missed.  
*One or more key need dates in the program schedule, but not critical path events, would be at least one month late; there are identified schedule workarounds that would be sufficient to keep the program critical path from being affected. There would be only a limited impact on the success of the program.*
4. **Significant:** Given that the risk is realized, the program critical path would be affected.  
*One or more events on the program critical path would be at least one month late. There are identified schedule workarounds that would be sufficient to meet major program milestones. The success of the program could be jeopardized.*
5. **High:** Given that the risk is realized, a key program milestone cannot be achieved.  
*Completion of a key program milestone would be late, and the success of the program would be in doubt. The slip requires a re-baseline of the program.*

Figure 4.10-11. Schedule Consequence Definitions



## FAA Cost Consequence Definitions

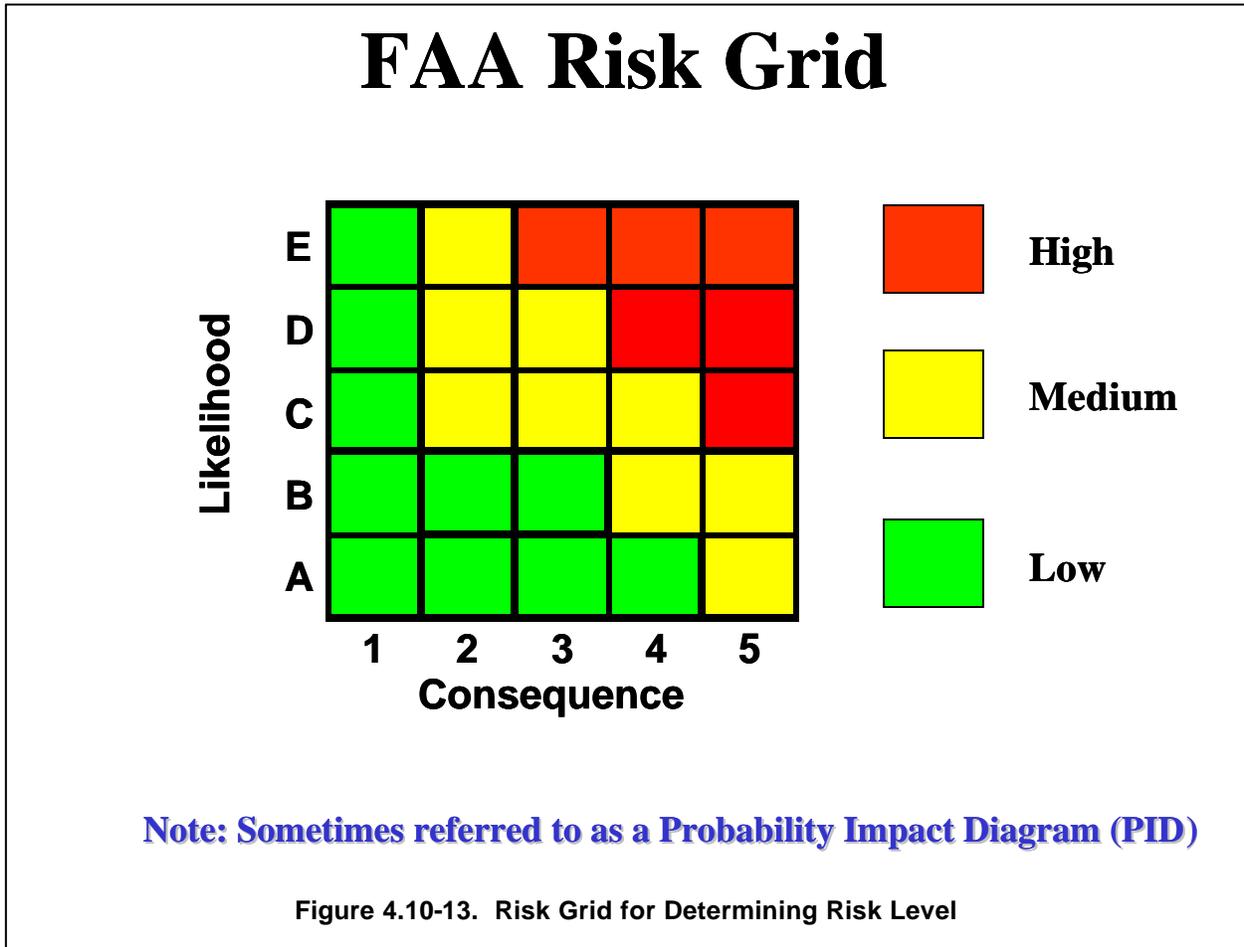
*Given the risk becomes real, what would be the magnitude of the impact on cost?*

1. **Low:** Given that the risk is realized, there would be minimal cost impact.  
*Program cost is not dependent on this issue. There would be no impact on the success of the program.*
2. **Minor:** Given that the risk is realized, the total costs, operating cost or unit production cost would increase by = 1%.  
*The program costs and/or the production unit cost would increase by = 1%. There would be no impact on the success of the program.*
3. **Moderate:** Given that the risk is realized, there would be a minor increase in financial need. The program costs, operating cost or unit production cost could increase above 1% up to = 5%.  
*The program costs and/or the production unit cost would increase above 1% to = 5%. There would be only a limited impact on the success of the program.*
4. **Significant:** Given that the risk is realized, the total costs, operating cost or unit production cost would increase by above 5% to = 10%.  
*The program costs and/or the production unit cost would increase above 5% to = 10%. The success of the program could be jeopardized.*
5. **High:** Given that the risk is realized, the total costs, operating cost or unit production cost would increase by greater than 10%.  
*The program costs and/or the production unit cost would increase by greater than 10%. The success of the program would be in doubt.*

Figure 4.10-12. Cost Consequence Definitions

**4.10.3.2.3 Risk Level Determination**

The likelihood and consequence are considered to be independent, but are tied to the same event. They are mapped into a risk grid (sometimes referred to as a Probability Impact Diagram (PID)) to determine the individual risk level (e.g., high (red), medium (yellow), or low (green)) as shown in Figure 4.10-13. This mapping facilitates prioritization and trend analyses of risks throughout the life of the program. Use of a color code for each risk level definition supports



effective communication of program health internally and externally, and it is recommended that it be determined early in the life of the program. In some instances, a “risk value” can be computed as the product between the likelihood value and the consequence. This metric is then used to establish a rough priority ranking of the risks.

The construct of a strong risk statement is presented in subsection 4.10.3.1.3 above. As shown in Figure 4.10-13, the “if” portion of the statement maps to the vertical axis of the grid shown, and the “then” portion maps to the horizontal axis. If the risk statement is framed properly, the assessment and subsequent decisions on how to deal with the risk become straightforward.

Risk level definition “**High**” (red) is likely (a high probability) to cause significant disruption of schedule, increase in cost, or degradation of performance. Concerted and continual emphasis and coordination may not be sufficient to overcome major difficulties. “**Medium**” (yellow) may cause some disruption of schedule, increase in cost, or degradation of performance. Special emphasis and close coordination is probably sufficient to overcome difficulties. “**Low**” (green) or

“Basic” (OMB terminology for the same level) has little potential for disruption of schedule, increase in cost, or degradation of performance. Normal emphasis and coordination is probably sufficient to overcome difficulties. The threshold for differentiating between high, medium, and low may change slightly from program to program, but not from risk to risk on the same program or organization.

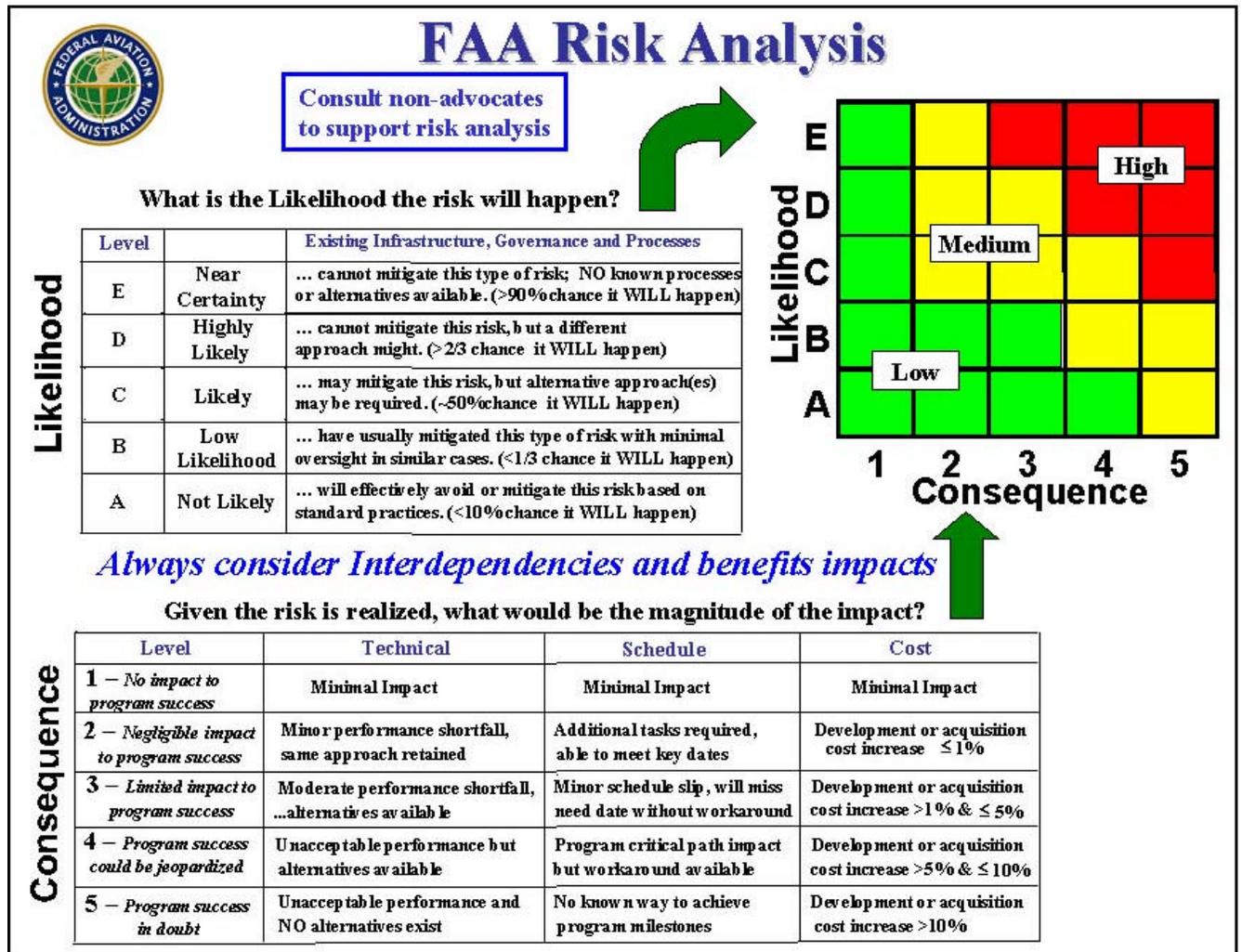


Figure 4.10-14. Risk Analysis



The color coding on this grid is also used to communicate management’s threshold of risk acceptability. For acquisition or development programs, this threshold is usually the line between green and yellow. While development programs are focused on maturing a point solution for a requirements set, research is aimed at determining the feasibility of an approach or technology. For research programs, the level of acceptability is typically defined as the threshold between yellow and red because the success criteria of research do not require the same degree of granularity as development. The degree of risk level acceptance and the actions required to reduce a risk below that level shall be detailed in the Risk Management Plan.

Figure 4.10-14 summarizes how the consequence and likelihood are consolidated to define the risk level.

Various technical communities employ risk analysis techniques or methodologies specific to their domain. They portray their conclusions and recommendations as grids similar to that shown in Figure 4.10-14; but the scales vary from 3 x 3 to 10 x 10 with many variations in between. It is recommended that the representation a given specialty community (such as Safety or Information Security) uses to draw conclusions be suited to its particular situation. However, the criteria used and portrayal of a community's conclusions and/or recommendations shall be consistent with the program or organizational view of risk. Figure 4.10-15 illustrates this correlation for the Information Security Engineering risk elements in Figure 4.8.6-5 (see Section 4.8.6, Information Security) and the basic risk elements discussed in this section. Regardless of the steps/methodologies used by a specialty knowledge domain, all risks need to be portrayed to management on the same basis (see Section 4.10.3.5 below) to allow for effective decisions on the application of risk reduction resources. However, the basic conclusion(s) reached by the specialty community must be preserved in any translation into a common program reporting format.

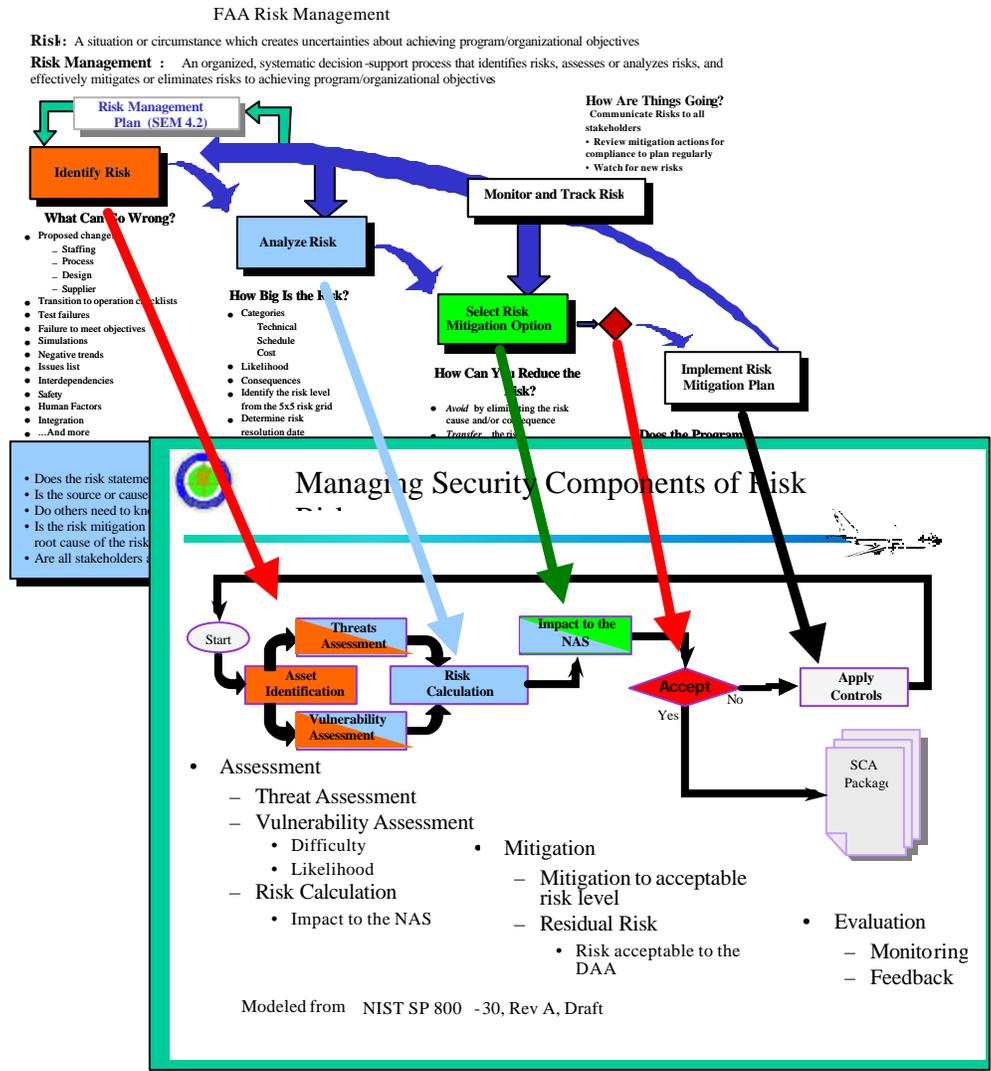
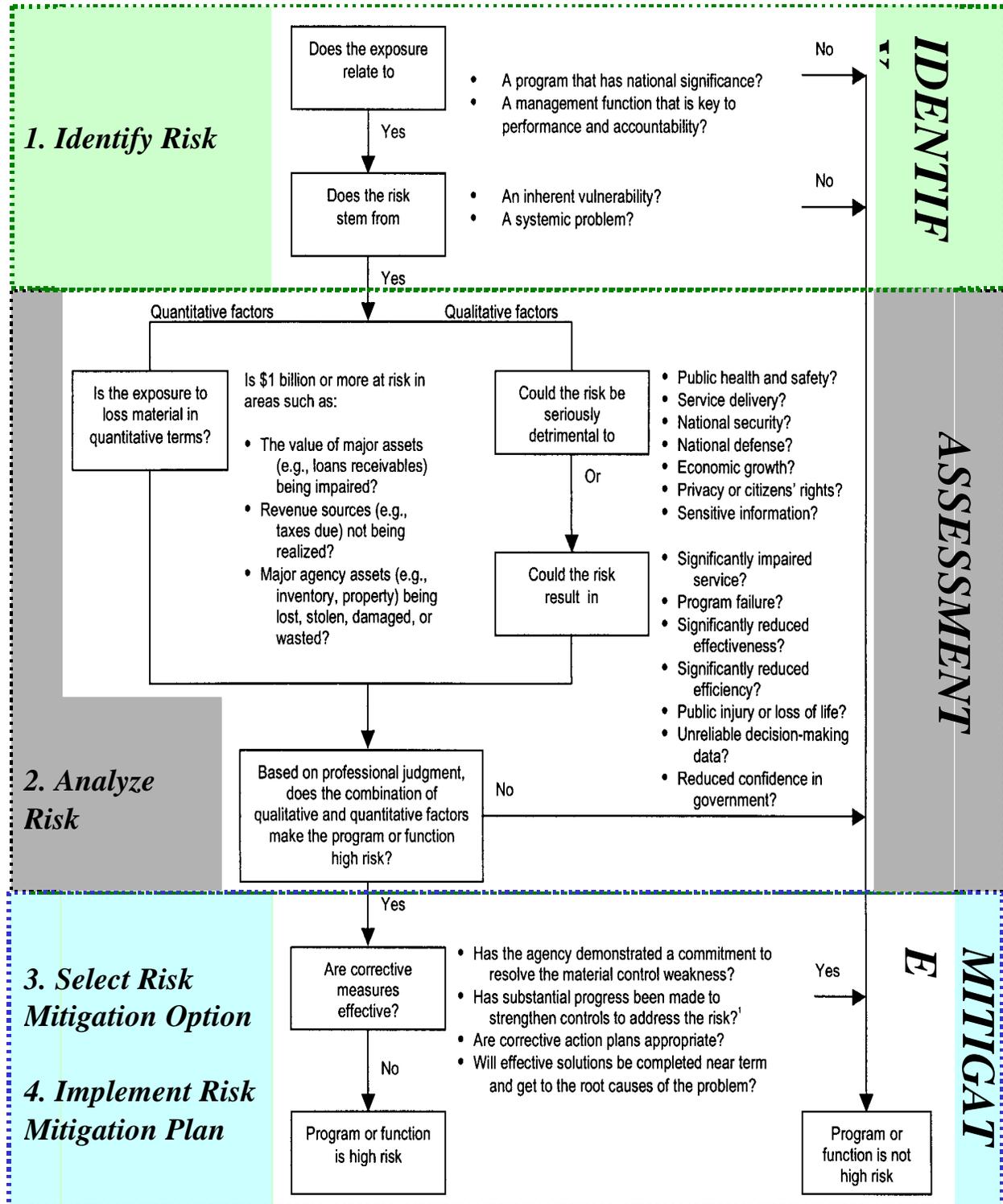


Figure 4.10-15. Correlation of Risk Management With Information Security Methodology

**GAO Risk Assessment Process/Criteria**



GAO process requires examination of risk and the development of a mitigation effort. Shown is Figure 5 of GAO/OCG-00-12, Page 9. (August/2000).

Figure 4.10-16. Correlation of GAO Recommendations With FAA Risk Management

The Government Accountability Office (GAO) [formerly the General Accounting Office] has also defined a process to handle risk in a report issued in 2000 (see item 16 in References at the end of this section). It contains the same elements in the FAA Risk model except the track and control step. Figure 4.10-16 shows the correlation between the two approaches and demonstrates how the GAO recommendations are satisfied with the process described in the FAA System Engineering Manual (SEM).

#### 4.10.3.3 Task 3: Select Risk Mitigation Option (*Satisfies iCMM BP 13.05 criteria*)

The objective of risk mitigation or risk reduction efforts is to implement appropriate and cost-effective risk mitigation plans to reduce or eliminate the risks. Appropriate risk mitigation techniques are selected and mitigation actions are developed, documented, and implemented. Risk mitigation handling (planning, implementation, and tracking) is the core of risk management. Risk mitigation 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 a combination, of the following strategies:

- Avoidance
- Control
- Assumption
- Transfer (sometimes referred to as “influence”)
- Research and Knowledge

**Avoidance** is a strategy to avert the potential of occurrence and/or consequence by selecting a different approach or by not participating in the situation that potentially generates the risk. This technique may be pursued when multiple technical or programmatic options are available. It is more likely used as the basis for a go/no-go decision at the start of a program. Some examples are selection of state-of-the-practice rather than state-of-the-art technologies and prequalification of suppliers. The avoidance of risk is from the perspective of the overall program/project, which includes the stakeholders, contractors, and execution groups. Thus, an avoidance strategy is one that involves all of the major parties to the program/project and permits a program/project-wide avoidance of the risk.

**Control** is a strategy of developing options and alternatives and taking actions that lower or eliminate the risk. This is the most common approach used to handle risks. The objective of this strategy is to take action or make a decision to lessen the probability of occurrence and/or the impact if the risk were to occur. Examples include new concepts, additional technical analysis, redundant systems and/or components, and alternate sources of production.



Refer to Table 4.10-6 for more information on choosing control as the risk handling approach.

Table 4.10-6. Sample Risk Handling Strategies

Typical Risk Control/Mitigation Approaches
<ul style="list-style-type: none"><li>• Multiple development efforts</li><li>• Extensive alternative design studies</li><li>• Trade studies — technological development verses operational impact</li><li>• Early prototyping</li><li>• Incremental/Evolutionary/Spiral development</li><li>• Technology maturation efforts</li><li>• Robust design</li><li>• Reviews, walkthroughs and inspections</li><li>• Open Architecture and Systems</li><li>• Use of standard items (COTS)/software reuse</li><li>• Use of engineering mockups</li><li>• Modeling and simulation</li><li>• Key parameter control boards</li><li>• Manufacturing screening (Environmental Stress Screening)</li></ul>

**Assumption** is simply accepting the likelihood/probability and the consequences/impacts associated with a risk's occurrence without engaging in any special efforts to control it. Assumption is usually limited to low risks. This is a program/senior management option, not a practitioner option. FAA practice for investment programs is to develop mitigation plans for all medium and high risks. However, the actions required to address individual risks shall be contained in the governing RMP.

**Transfer** is a strategy to shift the risk to another area, such as another requirement, an organization, a supplier, or a stakeholder. Examples include reallocating requirements, securing supplier product warranties, and negotiating fixed-price contracts with suppliers. Note that at the program or higher organizational level, the risk remains; the transfer of the risk is accomplished primarily to optimize the overall program risk and to assign ownership to the party most capable of reducing the risk. Risk cannot be transferred unless the recipient agrees to accept the risk. It is possible that the risk level may change as a result of the risk transfer.

**Research and Knowledge** may mitigate risk through expanding research and experience. Since risk arises from uncertainty and inexperience, it may be possible to effectively mitigate risk simply by enlarging the knowledge pool, leading to reassessment that reduces the likelihood of failure or provides insight into how to lessen the consequences.

At this point, several alternatives for mitigating the risk have been identified and analyzed for selection of the preferred approach. 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. 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. The mitigation steps are the major milestones of the mitigation plan. 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 (see Figure 4.10-6) have known risk mitigation strategies. These strategies need to be included in the trade studies 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, which is available at <http://www.faa.gov/aua/resources/COTS>.



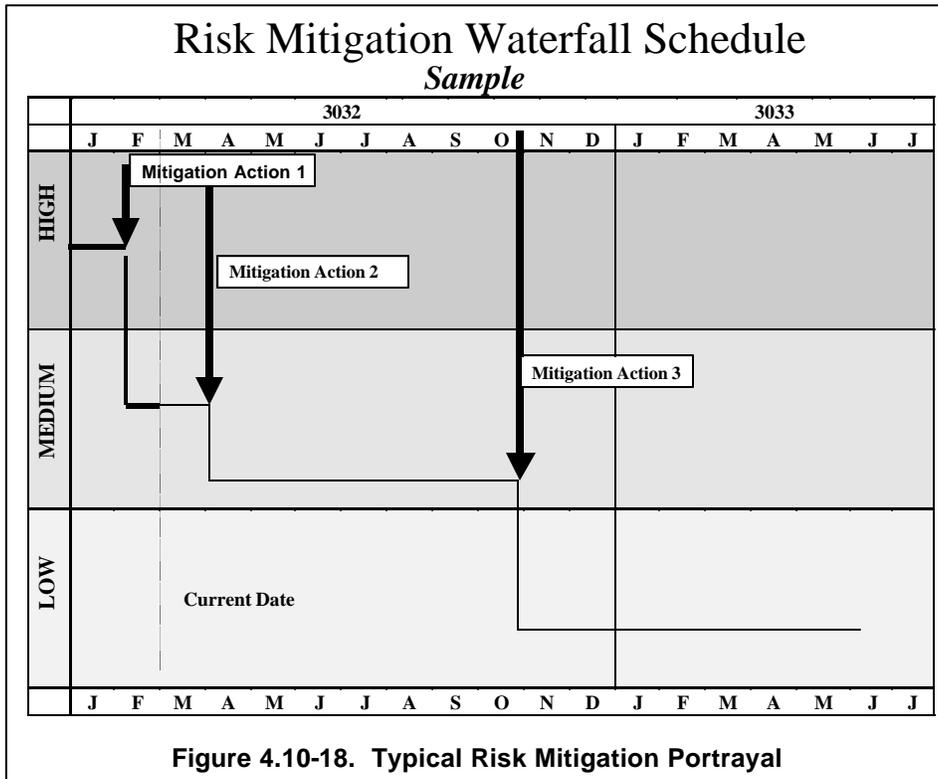
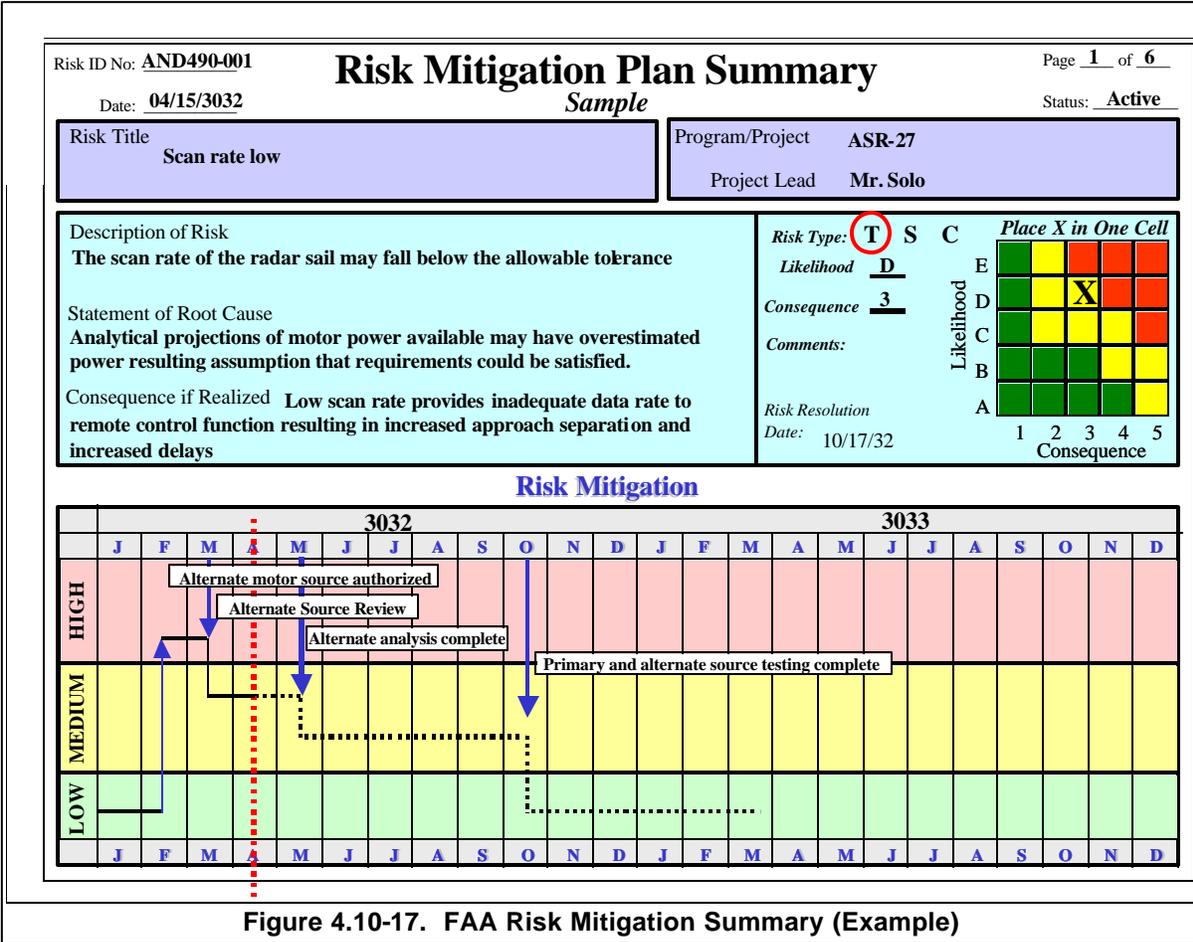
Trade study techniques may be performed to help select the preferred risk mitigation plan. While the proper criteria and their weights for each analysis are dependent on the risks to be mitigated, it is recommended that the following considerations be included:

- Does the option mitigate the likelihood or consequence of the risk?
  - Does the option fit within program/organization’s scope?
  - Is the option easy to implement?
  - Are new risks avoided or introduced as a result of the mitigation?
  - What is the cost of mitigation?
  - What is the schedule for mitigation?
  - Is the recommended course of action an acceptable approach to management?
- While this implies some limitations on the choices considered, it should **NOT** preclude an approach not used before **IF** solid rationale can be offered to support it.

The risk level is the first criterion used to determine the need for a risk mitigation plan. As specified in the 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 those responsible for plan implementation 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 subsection 4.10.3.1.3). 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 (Figure 4.10-17) 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. The expected impact of each mitigation event on risk level may be projected using a format similar to that of Figure 4.10-18 (a waterfall, or “burn down,” chart).



The risk mitigation plan becomes the basis for monitoring success in reducing each risk to an acceptable level. The plan includes, but is not limited to, the following:

- A description of the risk for which the plan applies
- Mitigation approaches which detail the specific actions that are planned to reduce the risk or eliminate it. It is recommended that these actions be event based, integrated into a schedule, and have associated with each of them:
  - The decision point or trigger, past or future, that initiates the action or group of actions
  - Resources required to execute the actions (including personnel, capital equipment, facilities, procured equipment)
  - Measures of success to be used for the planned actions or group of actions
  - Fallback options or contingency plans (if any)
  - Planned completion dates of the actions
- Risk mitigation metrics
- The Risk Worksheet (Figure 4.10-7)
- The initial Risk Mitigation Plan Summary (Figure 4.10-17)
- The Risk Mitigation Waterfall Schedule (Figure 4.10-18)

A risk mitigation plan must be periodically evaluated to determine its effectiveness. This analysis is performed in the same manner as initial analysis for the risk. The set of templates used for analysis of the risk may also be used to determine the mitigation in the risk level following completion of each major action or group of actions. The regular reassessment of the risk and performance-to-plan using a fixed set of criteria provides a consistent analysis of the impact to the program.

An effective technique is to indicate in advance how successful completion of the actions outlined in the Risk Mitigation Plan affects the risk. Not all actions have a comparable impact. Some actions or decisions provide the basis for others to be effective. In contrast, certain events, actions, or decisions have a fundamental impact on the level of risk remaining, both from a positive and negative perspective. A “best practice” can be illustrated when the mitigation plans for several of the examples of strong risk statements discussed in subsection 4.10.3.1 are reviewed (details have been changed for illustrative purposes):

Our first example of a strong risk statement (Risk #216) stated: “If either the multiple SMR SAT completion or the start of the ASDE-X Safety Logic Optimization by July 15, 2006, is delayed in any way, then the commissioning of the new Atlanta ATCT and the IOC date of May 1, 2007, will be delayed, which will not meet the terms of the AT/NATCA MOU.”

This was initially assessed as a high (red) risk, which means that effective action needed to take place to reduce it. The mitigation strategy recommended and accepted was threefold: (1) to monitor the sensor and safety logic development progress with each system enhancement, (2) manage the results to realistic expectations, and (3) pursue a single sensor configuration in lieu of multiple sensors to reduce complexity and associated cost/schedule. To implement this strategy, the program put the following actions and schedule in place:

- 12/01/05: Monitor Safety Logic Test and Development activities in MCO. Note: Unsuccessful IOT&E at MCO could impact Atlanta Safety Logic testing start.
  - 02/26/06: Track schedule of Single SMR Optimization to ensure that it is on schedule. Measure remaining schedule to see if allotted time available is sufficient to complete Multiple SMR optimization. If not, by 5/13/06, accelerate optimization efforts of FAA field personnel and vendor.
  - 05/13/2006: Multiple SMR optimization start — poor performance will trigger single SMR contingency.
  - 07/2006: Safety Logic optimization start *(trigger to reassess risk)*.
  - 10/2006: Formal SAT start *(trigger to reassess risk)*.
  - 02/2007: Safety Logic optimization and test *(trigger to retire risk)*.
- (Risk last reviewed 11/2005)

In our second example (Risk # 305), the risk statement read: “If the Safety logic design and associated performance does not meet the operational expectations at Orlando International (MCO), then the ability to achieve ISD and deploy at other sites per the deployment schedule will be at risk with continued potential of accidents caused by runway incursion incidents at those locations.”

This was assessed as a high (red) risk. A mitigation strategy to define requirements for operational expectations and conduct software code reviews, data analyses, and Operational Tests (OT) to assess system performance was developed, and the following detailed actions were put in place:

- 03/23/2006: Define operational expectations.
- 07/27/2006: Collect operational data for future data analysis.
- 10/29/2006: Conduct shadow operations with users to identify areas of concern.
- 02/14/2007: Identify design and adaptation changes to improve system performance *(trigger to reassess risk)*.
- 03/2007: Conduct additional shadow operations testing to identify needed improvements.
- 05/06/2007: Conduct operational test to assess performance and identify potential system changes *(trigger to reassess risk)*.
- 07/8/2007: Use Tech Center lab to analyze results from shadow operations and OT.
- 07/2007: Conduct software code reviews to verify functionality.
- 09/2007: Conduct full IOT&E at MCO *(trigger to retire risk)*.

(Risk last reviewed 11/2005)

In our final example, (Risk # 389), a medium (yellow) risk level was assigned to the risk statement: “If adjustments are not made to the installation schedule to accommodate aggressive intervals for key activities, the ASDE-X system may be in jeopardy to meet the

Operational Required Date at Seattle International in time to support the decommissioning of ASDE-3 in August 2007, as required in the MOU with the Port of Seattle.”

The plan adopted involved compressing the remaining available schedule by adding resources. The details of this plan involved the following actions:

- 10/2005: The resources assigned to site preparation have been increased. A 3-person team was instituted for the months of April through October 2005, which helped to absorb loss of time for site preparation activities (i.e., added resources to the project instead of extending schedule) (**complete**).
- 10/22/2005: Site prep (**complete**).
- 04/2006: Optimization of Remote Units and SMR planned complete (**trigger to reduce risk rating**).
- 10/2006: IOT&E.
- 01/2007: Field performance evaluation complete.
- 06/2007: Achieve IOC (**trigger to retire risk**).

(Risk last reviewed 11/2005)

**Tip**

In addition to the attributes of a strong risk statement described in subsection 4.10.3.1.3, the characteristics of an effective mitigation plan illustrated in each of these examples include:

- A strategy or approach that traces directly to the problem statement, and, therefore, addresses the root cause of the risk rather than symptoms
- Defined and measurable actions that are integrated into the Integrated Master Schedule (IMS)
- Triggers to reassess risk level and progress to plan
- Currency of risk information (both status and date last reviewed)
- Interdependencies that impact the effectiveness of individual mitigations

The Risk Worksheet (Figure 4.10-7) guides the practitioner through the first three tasks in the Risk Management process: Identify, Analyze, and Develop mitigation planning to obtain a risk reduction decision. When a risk mitigation plan has been prepared, management reviews and approves it based on criteria defined in the RMP. The decision is reflected in the disposition blocks at the bottom of the Risk Worksheet.

#### **4.10.3.4 Task 4: Implement Risk Mitigation Plan (*Satisfies iCMM BP 13.05 criteria*)**

Once the organization decides on a risk mitigation approach and supporting actions, the decision shall be implemented and carried out effectively so that either risk likelihood or consequence, or both, are reduced to an acceptable level. Risk reduction implementation requires that the associated specific tasks be incorporated into the planning, scheduling, budgeting, and cost-accounting systems used by the program or in the implementing organization. Incorporating risk mitigation actions directly into the overall program schedule at a point where risk likelihood or consequence may be affected before a risk occurs keeps management and the program team/organization aware of the need to allocate resources (labor, materials, and possibly other resources) to accomplish the authorized risk reduction. The Risk Mitigation Plan Summary chart (Figure 4.10-17) is used as a means of reporting

progress in reducing risks. Each major event in the mitigation plan is identified along with how that event reduces the risk and to what extent.

Incorporating the risk mitigation plans and milestones into program and organizational processes and systems ensures that the risk and its mitigation plans may be monitored and tracked until the risk is eliminated, or the risk requires program modification. Risk mitigation plans may be documented starting with the Risk Worksheet (Figure 4.10-7) and a Risk Mitigation Waterfall Schedule (Figure 4.10-18). Mitigation activities are shared with and communicated to all stakeholders.

**4.10.3.5 Task 5: Monitor and Track Risks (Satisfies iCMM PA 14 criteria)**

Because risk is dynamic, continual attention of all involved is necessary regarding how the risk profile is changing based on events, decisions, and actions on the project. Reassessing currently managed risks is done on both a periodic and event basis to reflect current status of the risks as well as to identify and quantify new and emerging risks. The SE milestones and quality gates discussed in Integrated Technical Planning (Section 4.2) provide formal checkpoints for management insight into the risks as well as achievements to date. There will be additional opportunities for project personnel to periodically status risk as outlined in the RMP. New potential risks to the program may be identified at any time. Newly identified risks are analyzed using the same steps described in subsection 4.10.3.2.

## Program Risk Summary

*Sample few risks*

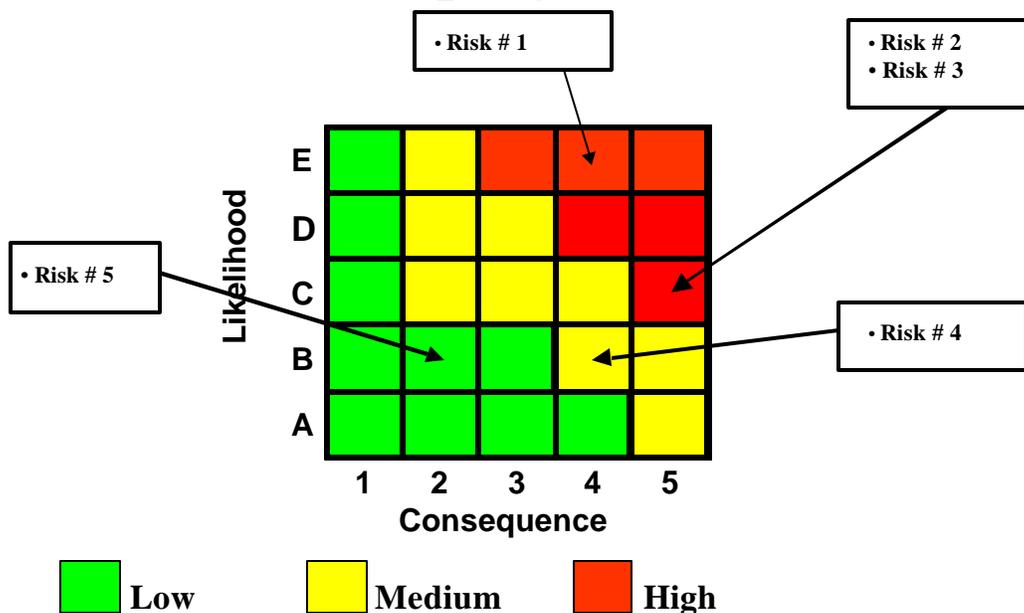


Figure 4.10-19. Aggregate Risk Grid

Steps in the risk-tracking process focus on providing program risk trends and status to the execution teams, interdependent activities, and program management. Actual performance of the planned mitigation actions is compared to the expected performance. The bold line on the Risk Mitigation Plan Summary “waterfall area” (see Figure 4.10-18) indicates progress made to date on the mitigation plan. Detailed cost and schedule tracking is done as part of the program

schedule and cost-tracking system. To ensure consistency across the program/organization, the governing RMP shall contain the management visibility requirements for the program. These requirements include reporting frequency and content.

A sample of a brief summary of all risks for a particular program (or team) with relatively few risks is displayed on an aggregate risk grid (or Probability Impact Diagram) shown in Figure 4.10-19. A standard reporting format shall be used (see Figure 4.10-20) to facilitate integration of risk information across projects and programs. It is recommended that the risk management plan also indicate the extent of required supporting detail, usually in the format of templates (see Figure 4.10-21). 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 (Figure 4.10-22). 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 (Figure 4.10-22, top) to lowest level tasks (Figure 4.10-22, bottom) allows program management to maintain appropriate risk visibility and also allows "drill down" to increasing levels of detail as the schedule view is expanded.

*(Extracted from PMR TEMPLATE)*

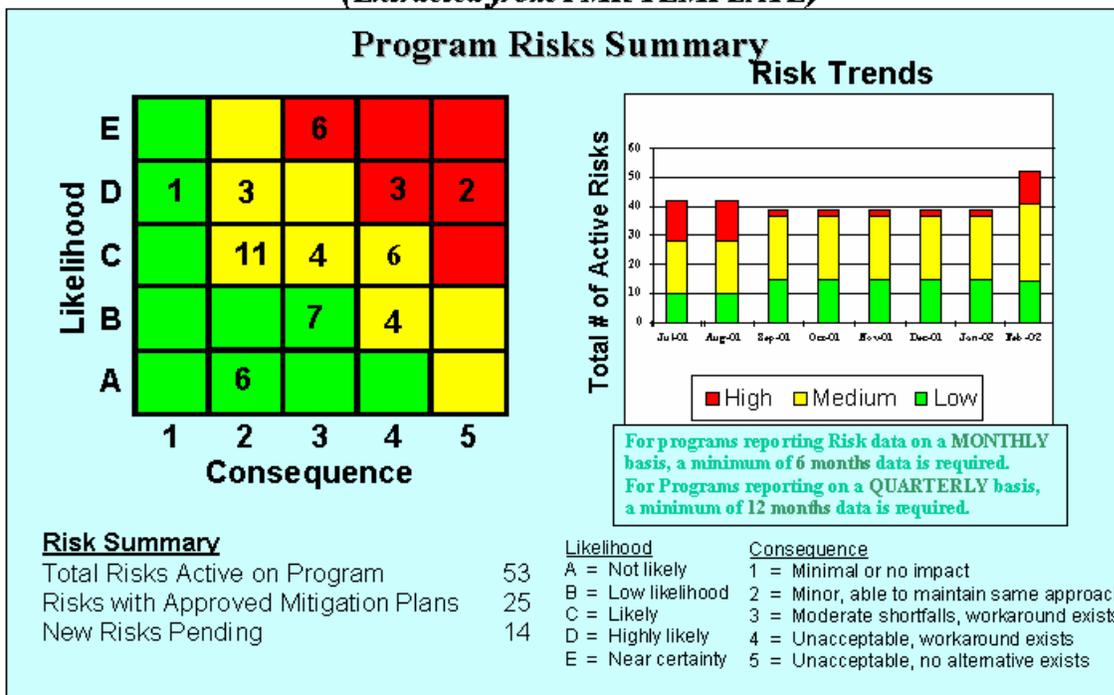


Figure 4.10-20. Standard Risk Reporting Format

(Extracted from PMR TEMPLATES) Program Risks

Risk Level	Risk #	Likelihood	Impact	Risk Type	Risk Item	Mitigation Strategy	Risk Mitigation Decision Date
H	46	E	4	TS	IF TSOs and ACs are delayed, THEN the standards will not support mandated deployment dates.	PT will work with industry to secure support	Jan-01
H	14	D	5	C	Airspace User Coordination – IF GA Aircraft users do not accept NEXCOM plan - Benefits for GA not sufficient to engender support - Low end GA Avionics costs too expensive	PT reps will meet with reps of the GA community to determine concerns and strategies for resolution of concerns.	Jun-02
H	30	D	5	C	IF Business case does not demonstrate ROI, THEN airlines won't equip.	PT will establish joint working group with industry to develop business case that industry can support.	Jul-02

List risk updates IN PROGRAM PRIORITY ORDER for each New, High Risk item (Red), and Significant Level Changes (High to Low &/or Low to High).

Likelihood  
 E = Near certainty  
 D = Highly likely  
 C = Likely  
 B = Low likelihood  
 A = Not likely

Consequence  
 1 = Minimal or no impact  
 2 = Minor, able to maintain same approach  
 3 = Moderate shortfalls, workaround exists  
 4 = Unacceptable, workaround exists  
 5 = Unacceptable, no alternative exists

**Risk Level:**  
 H - High    M - Medium    L - Low  
 → = same as last report  
 ↓ = down from last report    ↑ = up from last report

Risk Type

T = Technical  
 S = Schedule  
 C = Cost

*Note: There is a difference between a risk and an issue. If something is a certainty, it is no longer a risk and should be described as an issue and reported on the issues/concerns slide*  
**Initially each High risk should be briefed. Subsequently, any new or major change to a risk item should be captured on this slide. See attached proposed "Risk Management" (Attachment #1) for guidance on how to assess and report program risks.**

Figure 4.10-21. Template Formats

Integrated Program Schedule: summary level (top) and “drill down” to lowest level tasks

ID	Task Name	Risk	Start	Finish	2002				2003				2004		
					Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
1	Mission Analysis		10/1/99	10/5/99											
7	Investment Analysis		10/6/99	10/11/99											
17	Solution Development	High	10/11/99	3/22/07	█	█	█	█	█	█	█	█	█	█	█
18	Program management		10/12/99	10/12/99											
22	System Engineering	High	10/11/99	1/23/07	█	█	█	█	█	█	█	█	█	█	█
23	System Requirements and Definition		10/13/99	10/13/99											
25	Analysis, Design, and Integration	High	5/31/01	1/23/07	█	█	█	█	█	█	█	█	█	█	█
26	Enhanced Visual Approach - Level 1	High	3/6/02	9/24/03											
44	CDTI-Enhanced Flight Rules - Level 2	High	2/28/02	1/7/05											
70	CDTI-Enhanced Flight Rules - Level 3	High	10/20/03	1/23/07											
96	Terminal Area Multilateration Performance Evaluation	Medium	12/31/01	1/24/03											
113	Terminal Area Common ARTS Integration	High	5/31/01	6/21/04	█	█	█	█	█	█	█	█	█	█	█

Risk information displayed at summary task level in the program Integrated Master Schedule (IMS)

- High risk
- Medium risk
- Low risk

(bottom).

ID	Task Name	Risk	Start	Finish	2002				2003				2004		
					Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1	Qtr 2	Qtr 3	Qtr 4	Qtr 1
1	Mission Analysis		10/1/99	10/5/99											
7	Investment Analysis		10/6/99	10/11/99											
17	Solution Development	High	10/11/99	3/22/07	█	█	█	█	█	█	█	█	█	█	█
18	Program management		10/12/99	10/12/99											
22	System Engineering	High	10/11/99	1/23/07	█	█	█	█	█	█	█	█	█	█	█
23	System Requirements and Definition		10/13/99	10/13/99											
25	Analysis, Design, and Integration	High	5/31/01	1/23/07	█	█	█	█	█	█	█	█	█	█	█
26	Enhanced Visual Approach - Level 1	High	3/6/02	9/24/03											
27	Resolve concerns with data collection procedures	High	3/6/02	4/17/02											
28	Carrier #1 equipage	High	3/20/02	3/20/03											
29	Data collection period #1		4/17/02	7/10/02											
30	Metrics report #1		7/17/02	7/17/02											
31	Data collection period #2		7/17/02	10/9/02											
32	Metrics report #2		10/16/02	10/16/02											
33	Data collection period #3		10/16/02	1/8/03											
34	Metrics report #3		1/15/03	1/15/03											
35	Data collection period #4		1/15/03	4/9/03											
36	Metrics report #4		4/16/03	4/16/03											
37	Document 1% - 3% improvement in terminal arrival rat	Medium	4/16/03	5/7/03											
38	Decision Point - Does data support Level 1 equipage?		6/18/03	6/18/03											
39	Certify CDTI use during visual approach	Medium	6/18/03	9/24/03											
44	CDTI-Enhanced Flight Rules - Level 2	High	2/28/02	1/7/05											
70	CDTI-Enhanced Flight Rules - Level 3	High	10/20/03	1/23/07											
96	Terminal Area Multilateration Performance Evaluation	Medium	12/31/01	1/24/03											
113	Terminal Area Common ARTS Integration	High	5/31/01	6/21/04	█	█	█	█	█	█	█	█	█	█	█

Drill down capability – Risk information displayed for lowest level tasks; summary tasks show highest level of risk for any subordinate task

Figure 4.10-22. Risk Information Incorporated Into Program



Effective program management always involves examining cost and schedule during review of the progress of the program. Making risk information visible as part of the IMS through linkage with each WBS element affected ensures that risk information receives ongoing management attention. Integrating program risk data into the integrated master schedule fosters better, risk-based decision making in at least five ways:

- The need for separate risk reviews competing for the program manager's time and energy is eliminated.
- Integrating the risk information into the IMS effectively prevents isolation of the risk efforts from the mainstream tasks and program milestones. The risk profile of the program is presented as part of the overall management view of the program. As each decision point is reached, the risk information associated with that event or WBS element is portrayed, and hence shall be considered.
- The portrayal of program progress illustrated in Figure 4.10-22 alerts management to when a decision needs to be made and what that decision is. This provides visibility across the entire program *in advance* of impending decision points so that the necessary relevant information is provided in a timely manner to support an informed decision.
- OMB requires FAA investments to manage costs and schedules on a "risk-adjusted" basis. Integration of risk information provides objective evidence that schedules and costs accommodate the risks involved.
- Examination of the risks provides insight into mitigations that lead to pursuing potential opportunities.

Major FAA programs must submit yearly budget estimates with supporting justification for the investment in accordance with OMB Circular A-11 (Reference 22). 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 should 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 (2006) section 300.3).

Please note that the OMB terminology discussion of "risk contained in risk management plans" (A-11 (2006) section 300.4) refers to risk mitigation plans as discussed in this section of the FAA SEM.

#### **4.10.4 Outputs (*Satisfies iCMM Artifacts criteria*)**

Five major outputs of this process that directly influence the program and/or an organization's decisions are:

- Program Risk Summary (Figures 4.10-20 and 4.10-21)

- Risk Mitigation Plan Summary (Figure 4.10-17)
- Risk Mitigation Plans (see subsection 4.10.3.3)
- Aggregate Risk Grid (Figure 4.10-19)
- Risk Status

It is recommended that the Program Risk Summary, the Risk Mitigation Plan Summary, and the Program Risk Mitigation Progress charts be briefed at all regular program reviews. Management decisions are based on the above information. It is recommended that a complete status of a given risk be briefed when the risk is identified and immediately following the risk realization date. It is recommended that the Risk Mitigation Plans be handled as an integral part of program effort.

#### **4.10.5 Risk Management Tools**

The tools needed to implement this process include:

- Approved Risk Management Plan
- FAA Risk Worksheet
- Likelihood and consequence templates for a 5 x 5 PID tailored for the program
- Risk Mitigation Plan Summary
- A means to communicate results across a program (electronic mail, servers, etc.)
- A means to document the results of the process and manage the outputs (databases, spreadsheets, word processors, etc.)
- Analytical tool(s) to support risk analysis and tracking

##### **4.10.5.1 Analytical tools**

Analytic tools assist in the assessment and management of risk information. Tool capabilities can range from the simplistic to very complex. Use of a given tool is driven by the needs of the organization's risk management efforts.

If risk can be managed or tracked on an individual basis without a need for integration with other risk efforts, a number of choices are available within the organization's current desktop environment using either word processing or spreadsheet applications. Another choice is a database application, which provides additional features. An example of a standalone or individual user database tool is "Risk Radar" (a tool free to the government that may be used to generate many of the risk work products (see subsection 4.10-4)). A version of Risk Radar that incorporates the FAA templates and forms is available through the System Engineering Council (SEC) sponsored Introduction to FAA Risk Management course (SEC 410). This software is available free to all FAA programs (including contractors for use in supporting FAA programs). It requires MS Access 2000 and interfaces with MS Project 2000 for schedule linkage to the overall program IMS.

If the requirements in the RMP for capabilities that go beyond those described above (such as risk rollup to different organizational levels), then a risk tool suite with network and/or Web capability may be required. There are a number of commercially available tools available that provide an array of capabilities ranging from Web-based entry through organization-wide risk, analytical capabilities, and even opportunity management.

Analytic tools may be used for probabilistic analysis of schedule uncertainty or technical uncertainty. Critical Path Analysis tools may be used with the Integrated Program Schedule to regularly evaluate schedule risk. In a similar fashion, commercial applications (e.g., @RISK) may be applied to technical parameters (such as weight, latency, power, computer throughput) to establish confidence ranges. Results from these probabilistic analyses may support the overall risk analysis task of establishing a likelihood of occurrence. Details on use of probabilistic analysis are not covered here, but may be found in textbooks and technical papers that cover statistical analysis for risk management. For those investments that require an Exhibit 300 to be submitted to OMB, a comprehensive tool suite is under consideration at the time of publication of this update for FAA-wide application. A Risk Management capability is planned to be part of that standard tool suite, especially since schedules and budgets need to be “risk adjusted”.

#### **4.10.5.2 Risk Register**

The risk register (see example in Figure 4.10-23) is a listing of risk information associated with achieving program objectives. If risk registers are created and maintained by each project, a single composite register of all interdependency risk items shall be developed for the program. These registers are to be consistently used to monitor and track overall risk status within team meetings, program management reviews, and major program reviews. Immediately following identification and analysis of a new medium or high risk, or when a significant change occurs in a previously identified risk, changes shall be incorporated in the register and other documents and the new risk identified to stakeholders. The distribution list is to be established and documented in the RMP. Computer database systems may be needed to manage these outputs for large programs. Smaller programs may often be able to use desktop computer techniques. At a minimum, the following information shall be included in the risk register:

##### **4.10.5.2.1 Risk Register Identification and Creation/Update Date**

This is the name of the program risk item. Indicate the root cause of the risk in this section.

##### **4.10.5.2.2 Risk Identification Number**

This number is a code that identifies a unique sequence.

##### **4.10.5.2.3 Likelihood**

This is a figure of merit indicating the relative likelihood/probability that the identified risk will actually occur (Likelihood Template, Figure 4.10-9).

##### **4.10.5.2.4 Impact (Consequence)**

This is a figure of merit indicating the relative severity of consequences/impacts that could result if the identified risk did occur (Consequences Templates, Figures 4.10-10, 4.10-11, and 4.10-12, for examples).

##### **4.10.5.2.5 Risk Level/Change**

This is a single letter indicating the assessed risk an item as high, medium, or low (H, M, L) or, red, yellow, or green (R, Y, G) respectively. An arrow that indicates the direction that the risk has moved since the last revision to the risk register demonstrates the risk change.

##### **4.10.5.2.6 Risk Consequence Description**

This is a brief, well-stated description of the risk’s negative consequences.

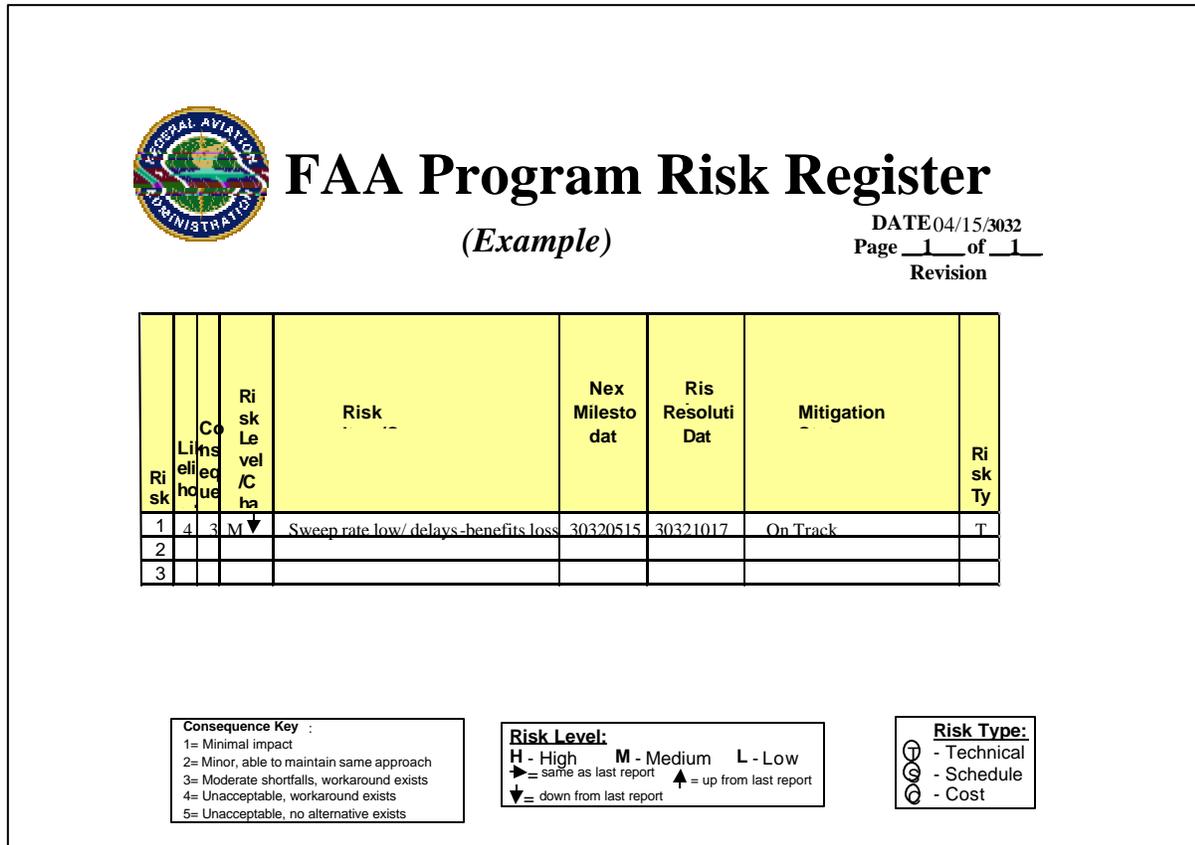


Figure 4.10-23. Risk Register

**4.10.5.2.7 Next Milestone Date**

This is the projected date at which the risk level converts to lower risk. This is traceable to the Risk Mitigation Plan Summary (Figure 4.10-17).

**4.10.5.2.8 Risk Realization Date**

This is **the date (or point in time) of the event that either makes the risk a real part of the program or eliminates the need to track the risk.** Early in the program, it may be difficult to predict an exact date, but a general timeframe needs to be developed. As the program matures, date realization occurs. It is recommended that these dates be reviewed regularly and be on the program master schedule.

**4.10.5.2.9 Mitigation Status**

The currently planned mitigation actions are defined, either explicitly or by reference.

**4.10.5.2.10 Risk Type**

The risk type designates if the risk is a cost risk, a schedule risk, or a technical risk (see subsection 4.10.3.1.1).

**4.10.5.2.11 Risk Mitigation Plan Status**

The teams regularly update and report the status of the risk mitigation plan for each risk being tracked that requires risk handling. Actions are initiated as required for mitigation plan activities that are not being accomplished. The risk status is also reviewed with program management on

a regular basis. A sample of a brief summary of all risks for a particular program (or team) is shown in a Program Risk Summary (Figures 4.10-19 and 4.10-20) for use depending on program size.

#### 4.10.6 Risk Management Process Metrics (*Satisfies iCMM PA 18 criteria*)

To be useful, Risk Management-related metrics must be focused on organization and/or project goals and success criteria. The metrics for risk management vary by organization and sometimes by project. Whatever measurements or statistics are used to help manage the project are the best metrics for that project. At the program level, these metrics measure program progress to plan. Earned Value Management (EVM) is an excellent set of measures to portray the extent of schedule and cost risk in a program. The variance to plan for either the Schedule Performance Index or Cost Performance Index may be used as a measure of risk on the program. The EVM reporting requirements in the OMB Exhibit 300 provide a ready means to capture risks of this nature. Technical or performance risk may be measured by using Technical Performance Measures. The projected and/or actual variance to performance requirements is a measure of technical risk. At a lower level, metrics for the Risk Management process itself may include:

- **Total active high risks, total active medium risks over time.** The objective is to provide visibility into risk trends over time.
- **Percent of risks (medium and high) with approved mitigation plans.** The objective is to measure the effectiveness of handling the risks requiring action.
- **Average time span of overdue mitigation activities.** The objective is to measure the effectiveness of meeting mitigation plan schedules.
- **Aging of active risk records.** The objective is to gain insight into the currency of the risk database.
- **Number of risks past their realization date.** The objective is to provide an indicator of the effectiveness to handle risks in a timely manner.

#### 4.10.7 References

1. U.S. Air Force, Air Force Materiel Command. *Risk Management*. Pamphlet 63101. AFMC, 09 July 1997.  
[http://www.sm.nps.navy.mil/mn3331\\_core/Calendar/Week6/Readings6/Risk\\_Mgt/US\\_AF\\_Risk\\_Mgmt\\_Guide.doc](http://www.sm.nps.navy.mil/mn3331_core/Calendar/Week6/Readings6/Risk_Mgt/US_AF_Risk_Mgmt_Guide.doc)
2. American National Standards Institute/Electronic Industries Alliance. *Processes for Engineering a System*. ANSI/EIA-632-1998, pp. 11, 13, 14, 17, 30, 33-4, 45, 49, 52, 67, 75, 77, 81, 96, 109. Requirement 24.
3. Blanchard, Benjamin S., and Walter J. Fabrycky. *Systems Engineering and Analysis*. Third edition. Englewood Cliffs, NJ: Prentice Hall, 1998, pp. 657-661.
4. Conrow, Edmund H. *Effective Risk Management*. Reston, VA: American Institute of Aeronautics and Astronautics, Inc., 2000. <http://www.risk-services.com/aiaabok1.htm>
5. Department of Defense. *Transition from Development to Production*. DOD 4245.7-M. Chapter 9-8. Washington, DC: U.S. Department of Defense, September 1985.
6. U.S. Department of Transportation. *Departmental Guide to Risk Management Planning*. DOT H 1350.252. Washington, DC: U.S. Department of Transportation, 22 May 1999.

7. Defense Acquisition University Press. *Risk Management Guide for DoD Acquisitions*. Fifth edition. Fort Belvoir, VA: Defense Acquisition University Press, June 2002. [http://www.dsmc.dsm.mil/pubs/gdbks/risk\\_management.htm](http://www.dsmc.dsm.mil/pubs/gdbks/risk_management.htm)
8. Defense Systems Management College. *Systems Engineering Management Guide*. Chapter 15. Fort Belvoir, VA: Defense Systems Management College, 1990.
9. Electronics Industries Alliance. *Processes for Engineering a System*. EIA 632. Arlington, VA: Electronics Industries Alliance, January 1999. 08/09/02. Rev. 99, Chg.H. <http://www.eia.org>
10. Federal Aviation Administration. *FAA Acquisition Management System*. Paragraph 2.9.14. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration. <http://fast.faa.gov/>
11. Federal Aviation Administration. *FAA Acquisition Program Baseline Template*. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration. <http://fast.faa.gov>.
12. Federal Aviation Administration. *FAA Orders 1900.47, 1050, 1600, 3900, and 1370.82*. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration.
13. Federal Aviation Administration. *Acquisition and Program Risk Management Guidance*. FAA P1810. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, December 1996.
14. Federal Aviation Administration. *Risk Assessment Guidelines for the Investment Analysis Process*. FAA Working Paper No. WP-59-FA7N1-97-2. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, July 1999.
15. Accounting and Information Management Division. *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making*. GAO/AIMD-10.1.13. Washington, DC: U.S. General Accounting Office, Accounting and Information Management Division, February 1997, Section 10.1.13.
16. Accounting and Information Management Division. *Information Security Risk Assessment*. GAO/AIMD-99-139. Washington, DC: U.S. General Accounting Office, Accounting and Information Management Division, August 1999.
17. U.S. General Accounting Office. *Determining Performance and Accountability Challenges and High Risks, Exposure*. Draft. GAO/OCG-00-12. Washington, DC: U.S. General Accounting Office, August 2000.
18. Grady, Jeffery O. *Systems Requirements Analysis*. New York, NY: McGraw-Hill, 1993, pp. 462-465. <http://www.mcgraw-hill.com/>
19. Grady, Jeffery O. *System Engineering Planning and Enterprise Identity*. Boca Raton, FL: CRC Press, 1995, pp. 168-177.
20. Grady, Jeffery O. *System Integration*. Boca Raton, FL: CC Press, 1994, p. 149.
21. Shish, Robert. *NASA Systems Engineering Handbook*. NASA SP-6105. Washington, DC: National Aeronautics and Space Administration, June 1995, pp. 37-44.
22. Office of Management and Budget. *Planning, Budgeting, Acquisition, and Management of Capital Assets*. OMB Circular No A-11, Part 7. Washington, DC: Office of Management and Budget, June 2006.

23. Project Management Institute. *A Guide to the Project Management Body of Knowledge* (PMBOK® Guide 2000 Edition). Chapter 11. Newton Square, Pennsylvania.
24. Ross, John F. *Living Dangerously: Navigating the Risks of Everyday Life*. Cambridge, MA: Perseus Publishing, 1999.  
<http://www.questia.com/PM.qst?action=openPageViewer&docId=85921102>.
25. *Best Practices: How to Avoid Surprises in the World's Most Complicated Technical Process —The Transition from Development to Production*. DON NAVSO P-6071, March 1986.
26. Forsberg, Kevin, Mooz, Harold, and Cotterman, Howard. *Visualizing Project Management: Models and Frameworks For Mastering Complex Systems*. Hoboken, NJ: John Wiley & Sons, Inc., 2005. 3<sup>rd</sup> Edition, pp. 223-253
27. International Council on Systems Engineering (INCOSE). *Systems Engineering Handbook: A "What To" Guide For All SE Practitioners*. INCOSE-TP-2003-002-03, Version 3
28. Navstar GPS Joint Program Office (JPO) - HQ Air Force Space Command (AFSPC). *Risk Management Operating Instruction*. GP Operating Instruction 63-1108 (Rev 1 Draft), xx Nov 2005.

## 4.11 Configuration Management

### 4.11.1 Introduction

Configuration Management (CM) is a formal system engineering (SE) management discipline that is defined as **“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.”**<sup>1</sup> The discipline provides a structured approach to identify, control, and maintain the configuration of a system/product during its lifecycle through establishment of baselines. 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.** CM enables organizations to ensure the integrity of their products through all lifecycle phases.

CM is the application of good, repeatable business practices to deliver a product that meets customers’ needs and enables maintenance of the product until end of service. CM includes five fundamental practices: (1) plan CM process, (2) identify baseline elements, (3) manage approved baseline elements, (4) verify and audit configuration, and (5) provide configuration status. These practices, along with data management, must be applied appropriately to maximize the benefits that can be obtained through CM. Each practice has standard supporting tasks that can be tailored to meet needs. These tasks are iterative in nature, in that CM provides a closed-loop process for managing change. Figure 4.11-1 is the high-level CM process overview.

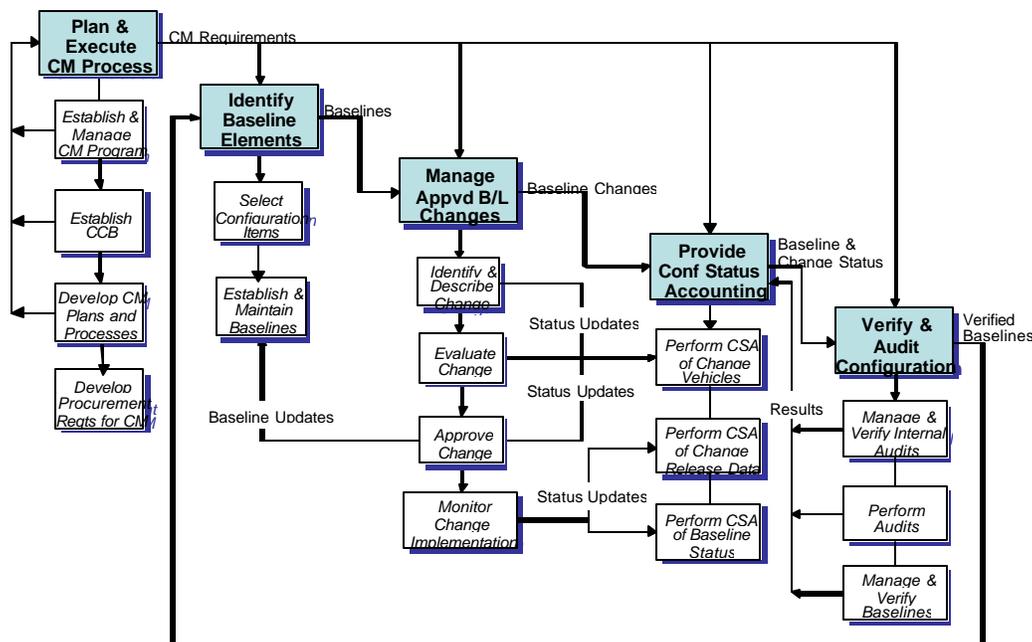


Figure 4.11-1. High-Level CM Process Overview

Applying CM to a product is progressive, which means that the initial concept of the product or service is documented, collaborated, and accepted. This adds further definition to the product

<sup>1</sup> ANSI/EIA-649-1998, National Consensus Standard for Configuration Management.

as it moves through its lifecycle. Product definition is expressed through establishment and maintenance of baselines. The Acquisition Management System (AMS) lifecycle phases discussed in this section are (1) Mission Analysis, (2) Investment Analysis, (3) Solution Implementation, and (4) In Service Management. To support determination of how CM should be applied to a product, it is important to understand and plan accordingly for the product nature, complexity, the user, product environment, and expected lifecycle.

To effectively manage a product through each of its lifecycle phases, government and industry best practices, which support the fundamental practices discussed in this section, need to be in place. These practices to conduct CM provide the means to plan and execute activities to reach the desired goals, which include delivering a quality product that meets the documented requirements, managing costs, meeting schedules, and enabling effective maintenance. These activities, when performed properly, provide a structured approach for managing systems and products throughout their lifecycles. subsection 4.11.3 details the CM process steps shown in Figure 4.11-1.

This section describes the fundamental principles of CM in the FAA. Details of how National Airspace System (NAS) CM is performed are defined and detailed through the AMS; FAA Order 1800.66, "National Airspace System Configuration Management Policy"; and other related process documentation.

Formal CM of NAS products is established for the lifecycle of a system through inclusion of CM requirements and activities in accordance with the AMS required documentation; contract documentation, such as the Statement of Work; and CM planning documentation. Designation of responsibility begins at approval of the functional baseline during the Investment Analysis phase. Responsibility includes establishing and maintaining a CM program for each product in accordance with FAA Order 1800.66. The order includes guidance on developing CM plans, processes, and procedures and allows for tailoring of CM processes.

The activities described below comprise the practices for successfully performing CM at the FAA. The national CM process is detailed in FAA Order 1800.66, Part Two, Section II, and should be used when tailoring processes to meet program needs. This tailoring may include the provision for performing change control outside a formal configuration control board (CCB) chartered by the NAS CCB, provided that the requirements for CM in FAA Order 1800.66 are met.

The main parts of this section are the key CM process inputs, both external and internal to the SE process; the CM process tasks; and key CM outputs and Data Management. The CM Process-Based Management chart, Figure 4.11-2, depicts the logical flow of information into and out of the CM process.



**Process:**

# Perform Configuration Management

**ID No.:**

4.11 (iCMM PA 16)

**Date:**

September 16, 2004

**Revision Date:**

August 30, 2006

**Next Higher Level Process:**

Perform System Engineering

**Process Owner:**

System Engineering Council

**Process Objective:**

Establish and maintain consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.

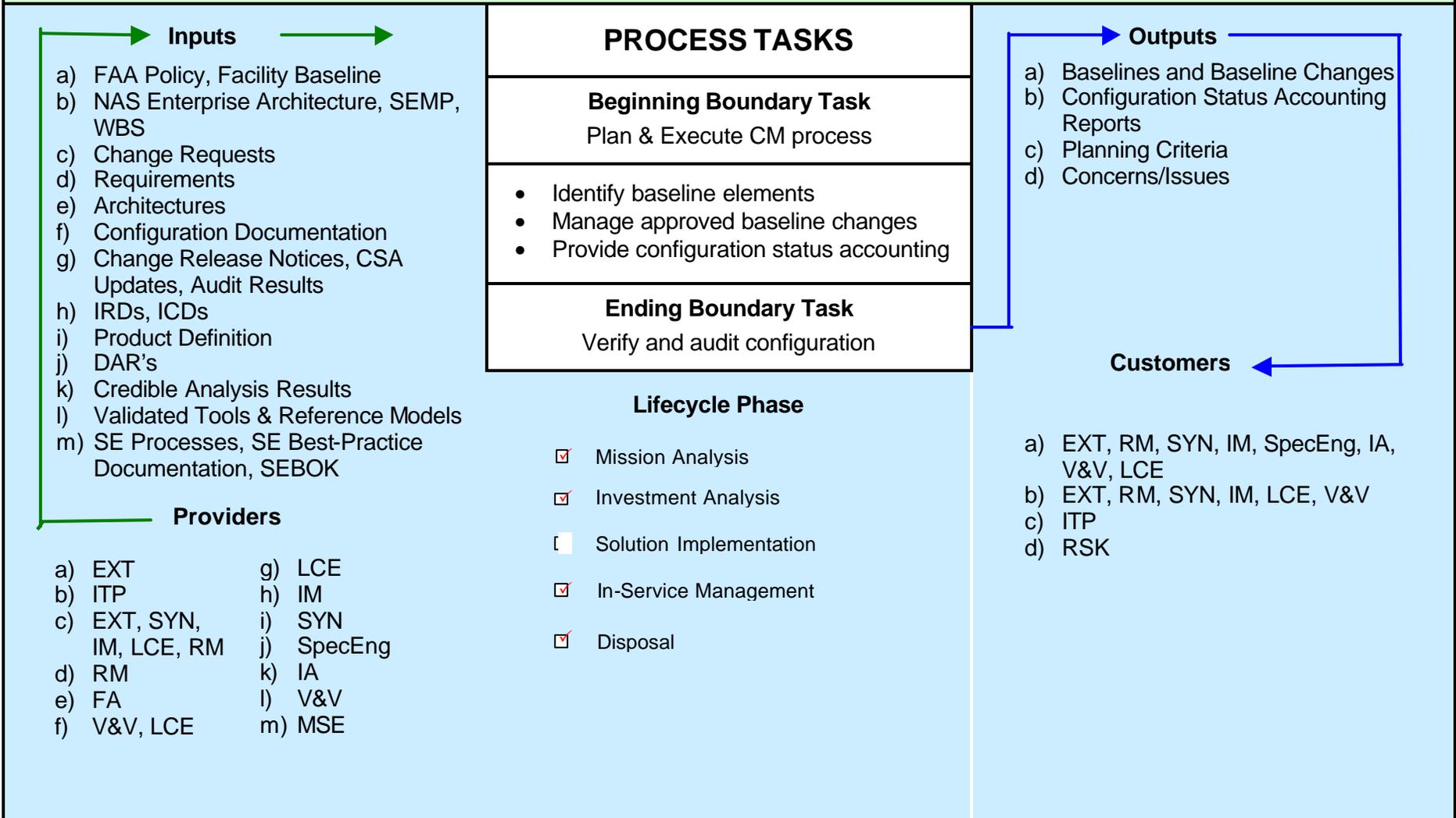


Figure 4.11-2. Configuration Management Process-Based Management Chart

### 4.11.2 Inputs

An input to CM is information that the CM process needs that provides direction; is the basis for or otherwise drives CM process activities; or requires action through one or more CM task areas.

#### 4.11.2.1 External

An external input is information provided to the CM process from outside the SE discipline process. The major external inputs to CM are as follows.

##### 4.11.2.1.1 FAA Policy

FAA policy and practices govern CM. The primary regulatory inputs to the CM process are:

- **FAA Order 1800.66.** CM policy, FAA Order 1800.66, prescribes the requirements and details the processes and procedures to perform CM of the NAS. The introduction of new products or services to the NAS or any changes to existing products or services must be accomplished in accordance with FAA Order 1800.66. This policy is a standalone document and is part of the FAA AMS.
- **AMS.** In addition to the CM policy, the AMS also addresses CM, such as developing CM criteria in the appropriate Program Plan(s).

##### 4.11.2.1.2 Change Requests

Outside parties use the CM process as a conduit to request changes to FAA-managed baselines. The requests can be:

- **Engineering Change Proposals (ECP).** The government uses ECPs to manage allocated and product baselines. The contractor's CCB must approve ECPs. This CCB is generally co-chaired by both the FAA and contractor representatives or, at a minimum, has FAA approval authority before implementation of the change.
- **Requests for Deviations and Waivers.** During product development or production, there may be instances in which deviations or waivers to requirements are needed. The contractor will submit requests to deviate (planned) from or waive (unplanned) a specific requirement as applicable. The contractor submits requests for deviation (RFD) or requests for waiver (RFW) to the FAA for approval using the form(s) referenced in the agreed-upon CM plan or contract documentation. RFDs/RFWs are generally temporary and are brought into compliance at a later time.
- **Contractor Change Vehicles.** Other contractor change vehicles affecting the change process must be documented in the contractor's/developer's approved CM plan.
- **Memoranda of Understanding (MOU).** MOU document agreement between FAA organizations or the FAA and an external organization when no formal contractual relationship exists between the parties. They may document a deviation in processes affecting standards or agreed-upon business practices or procedures, approval authority, or technical agreements (such as external

interfaces and data sharing). The CM process includes MOU as source data to be kept as part of the program documentation and used to drive, validate, and verify program activity as necessary.

#### 4.11.2.1.3 Facility Definition

Facility definitions are input by FAA facilities to the NAS CM process to establish and manage local facility baselines.

#### 4.11.2.2 Internal

Internal inputs are information provided to the CM process from within the SE discipline processes. The major internal inputs to CM are as follows.

##### 4.11.2.2.1 Integrated Technical Planning

Integrated Technical Planning (ITP) provides the framework in the form of plans and other planning information for executing the CM process on a program or within an organization. In particular, ITP furnishes the following:

- **System Engineering Management Plan.** The System Engineering Management Plan (SEMP) describes the SE work activity and the schedules associated with each task. Enterprise-level CM and related activity are captured and used by enterprise-level CM personnel to plan and execute activities affecting SE processes.
- **Configuration Management Plan.** Configuration Management Plans (CMP) describe program CM strategy, implementation activities, and standard practices for performing CM within a program. The ITP process (see Section 4.2) provides the strategy, activities, and practices for implementing CM within programs.
- **NAS Enterprise Architecture.** The NAS Enterprise Architecture (NASEA) is used as the basis for the overall baseline of how the NAS appears today. The NASEA is baselined and is the foundation of the Master Configuration Index (MCI). The MCI represents the current national configuration of the NAS and is the basis for the CM process relationships. Any changes to the NASEA or MCI must undergo formal change processing. The NASEA will be evaluated for possible changes when any other baseline changes that is traceable to the NASEA. If changes to the NASEA are required, then formal CM processing will be performed.
- **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.
- **Audit Results.** Configuration audit results are findings from formal configuration audits, such as functional and physical configuration audits. These findings may result in baseline changes or other actions required to meet baseline or contract requirements.

##### 4.11.2.2.2 Requirements Management

Requirements Management provides requirements to CM to be managed as follows:

- **Requirements.** NAS system requirements represent the highest level of requirements for the NAS. Lower level requirements for all new systems must be traceable from the top level. The CM ensures that all tasks required to maintain this traceability are executed.
- **Change Requests.** Any request for changes to the product definition is forwarded to CM for processing. The NAS Change Proposal (NCP), FAA Form 1800-2, is the coordination vehicle used internally to formally change NAS baseline documentation.

#### 4.11.2.2.3 Functional Analysis

For the CM process, the functional architecture presents a view of how the NAS provides the services detailed in the concept of operations through the NASEA.

#### 4.11.2.2.4 Synthesis

Synthesis furnishes CM products related to the solution being developed for formal release and control. In particular, Synthesis provides the following:

- **Product Definition.** The product definition provides Configuration Item (CI) descriptions to the CM process that are identified during the Synthesis process. The product definition documents all hardware configuration items and computer software configuration items (CSCI), including all documentation 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. The affected baseline determines the change vehicle to be used to update a baseline. CM uses the product definition to establish the product baseline.
- **Change Requests.** Any request for changes to the product definition goes to CM for processing. The NCP, FAA Form 1800-2, is the coordination vehicle used internally to formally change NAS baseline documentation.

#### 4.11.2.2.5 Interface Management

Interface Management provides interface requirements to CM to be managed as follows:

- **Interface Requirements Documents (IRD).** IRDs are submitted to the CM process for baseline establishment and control.
- **Interface Control Documents (ICD).** ICDs are submitted to the CM process for baseline establishment and control.
- **Change Requests.** Any request for changes to the interface definition of the product goes to CM for processing. The NCP, FAA Form 1800-2, is the coordination vehicle used internally to formally change NAS baseline documentation.

#### 4.11.2.2.6 Specialty Engineering

Design Analysis Reports provide information to assess proposed system baseline changes. They contain descriptions of a system's special characteristics, a list of requirements that were either validated or verified during analysis, residual risks, and candidate requirements found as a result of the analysis.

#### 4.11.2.2.7 Validation and Verification (V&V)

V&V provides documentation to CM to support establishment and control of product configuration(s) undergoing the V&V process. In particular, V&V provides the following:

- **Configuration Documentation.** Test article and test apparatus configuration documentation is submitted to CM for retention. This includes the configuration of test fixtures, jigs, test facilities, and tooling. Test article configuration documentation includes, among other items, whether the article was produced to production or test documentation or built on hard or soft tooling. The documentation is used to determine relevancy of verification results and for configuration audit purposes.
- **Test Results.** The CM process uses test results and inspection reports to document completion of product test milestones or to close actions, or as source data during the conduct of formal configuration audits.
- **Validated Tools and Reference Models.** All validated tools and reference models are submitted to CM to establish and maintain tool and reference model baselines.

#### 4.11.2.2.8 Lifecycle Engineering

Product and change coordination documentation is managed and controlled throughout the product's lifecycle. In particular, Lifecycle Engineering furnishes the following to CM:

- **Configuration Documentation.** Product documentation that is generated or modified during the product's lifecycle is submitted to CM. This includes elements of the product definition, such as configuration and interface control drawings, software design documents, version description documents, modification and maintenance records, and technical manuals.
- **Change Requests.** Any request for changes to the product baseline after delivery is forwarded to CM for processing. The NCP, FAA Form 1800-2, is the coordination vehicle used internally to formally change NAS baseline documentation.
- **Change Release Notices.** CM is a closed-loop process, meaning that a change is not considered closed until actual implementation has been completed. Documentation of completion includes change release notices that specify what has been changed, approval authority, and installation or implementation date. Change release notice information is a key component of configuration status accounting.
- **Configuration Status Accounting Report (CSAR) Updates.** CSAR updates provide the current status of MCI configuration items or work products from Lifecycle Engineering to keep CM status current. The supporting CM process can electronically generate and provide CSARs on demand or at scheduled intervals.

#### 4.11.3 Configuration Management Process Steps

This section identifies the CM process tasks and highlights the requirements for each activity.

#### **4.11.3.1 Step 1: Plan and Execute CM Process**

Planning for configuration management is key to successfully reaching program goals. Planning provides the basis for ensuring application of effective and efficient CM practices throughout each of the applicable SE processes. A discussion of all planning for CM appears in Integrated Technical Planning (Section 4.2), which describes the primary activities for implementing and maintaining CM.

##### **4.11.3.1.1 Step 1.1: Establish and Manage CM Program**

CM lifecycle management is the top-level CM activity used to implement the major CM principles over the program lifecycle. It includes coordinating and managing all tasks to implement CM principles and to conduct CM activities. CM planning determines the resources for CM activities throughout the lifecycle, establishes the mechanisms to perform the CM process, designates the responsibilities of the organizations performing the CM process, and ensures that control will be extended to vendors and contractors during equipment acquisition.

##### **4.11.3.1.2 Step 1.2: 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 ensures the functional and operational integrity of a baseline through establishment and enforcement of effective change management and control practices and processes.

Established by the FAA Administrator as the highest ranking CCB, the NAS CCB has authority to charter subordinate CCBs as necessary.

The service unit typically develops its CCB charter and operating procedures upon assignment of a NAS program or programs. Each CCB develops operating procedures according to its specific mission and needs. FAA Order 1800.66, paragraph 3.2.1.5, provides requirements for developing and maintaining CCB charters and operating procedures. Additionally, samples of current CCB charters and operating procedures are on the CM Web page (<http://www.faa.gov/cm/>).

##### **4.11.3.1.3 Step 1.3: Develop CM Plans and Processes**

CM plans and processes are to be documented in accordance with Section 4.2 (Integrated Technical Planning). Additional documents may be useful depending on the complexity of the CM tasks. Refer to FAA Order 1800.66, paragraph 3.2.2.1, for guidance on the specific requirements for CM planning.

##### **4.11.3.1.4 Step 1.4: Develop CM Procurement Requirements**

CM requirements of a proposed procurement are determined through reviews of procurement and planning documentation. CM deliverables must generally support management of the product during the contract and the maintenance philosophy for the procurement. Ensure that these identified requirements are incorporated into the statement of work and are itemized in contract deliverables. Additionally, review proposal responses to determine whether they meet the CM requirements and participate in post-award conferences to ensure that all parties involved have a common understanding of contract CM requirements and to resolve any issues.

#### **4.11.3.2 Step 2: Identify Baseline Elements**

This activity includes identifying associated work products, establishing and maintaining requirements on work products and services that result from the CM process, and

establishing requirements for controlling changes to those work products. Identifying these products provides the means to establish and maintain baselines. Systems/products are identified through SE, Integrated Technical Planning, and Synthesis processes. Key work products requiring management approval or concurrence include concepts of operation, plans, electronic data, and automated support tools.

#### 4.11.3.2.1 Step 2.1 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. Product attributes are applied to hardware, software, firmware, and their associated documentation. These attributes mature through each of the lifecycle phases and, at key milestones during those phases, are validated and incorporated into the baseline.

##### 4.11.3.2.1.1 Select Configuration Items (CI)

A CI ***is an aggregation of hardware, software, processed materials, services, or any of its discrete parts that is demonstrated for CM and treated as a single entity in the CM process.*** Selecting CIs separates the elements of a system or product into individual subsets to manage their development and subsequent change. Designating CIs for FAA CM usually occurs at the major subsystem levels of the WBS or to critical items, lowest replaceable units (LRU), and releasable software code elements. The process steps for selecting CIs in the FAA are as follows (see FAA Order 1800.66, paragraph 3.3.2.1):

- Establish program and program identification
- Plan acquisition strategy
- Select configuration items
- Update Plans

##### 4.11.3.2.2 Step 2.2 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. A baseline is “an agreed-to description of the attributes of a product at a point in time, which serves as a basis for defining change.”<sup>2</sup> The baseline includes a specific revision or version of approved and released documents, sets of documents, or electronic files (software and data) that serve as the basis for managing change. Formal baselines are established at designated times during each of the lifecycle phases, which appear in Figure 4.11-3.

Following are typical baselines that are established for an acquisition program. Because of NAS complexity, the FAA also maintains an enterprise-level, or NAS functional, baseline, which represents the top-level requirements for the NAS overall. Other FAA-unique baselines include the operational and facility baselines that are described below.

---

<sup>2</sup> ANSI/EIA-649-1998, National Consensus Standard for Configuration Management.

Figure 4.11-3 represents the product development process and the key CM milestones for baseline establishment and validation.

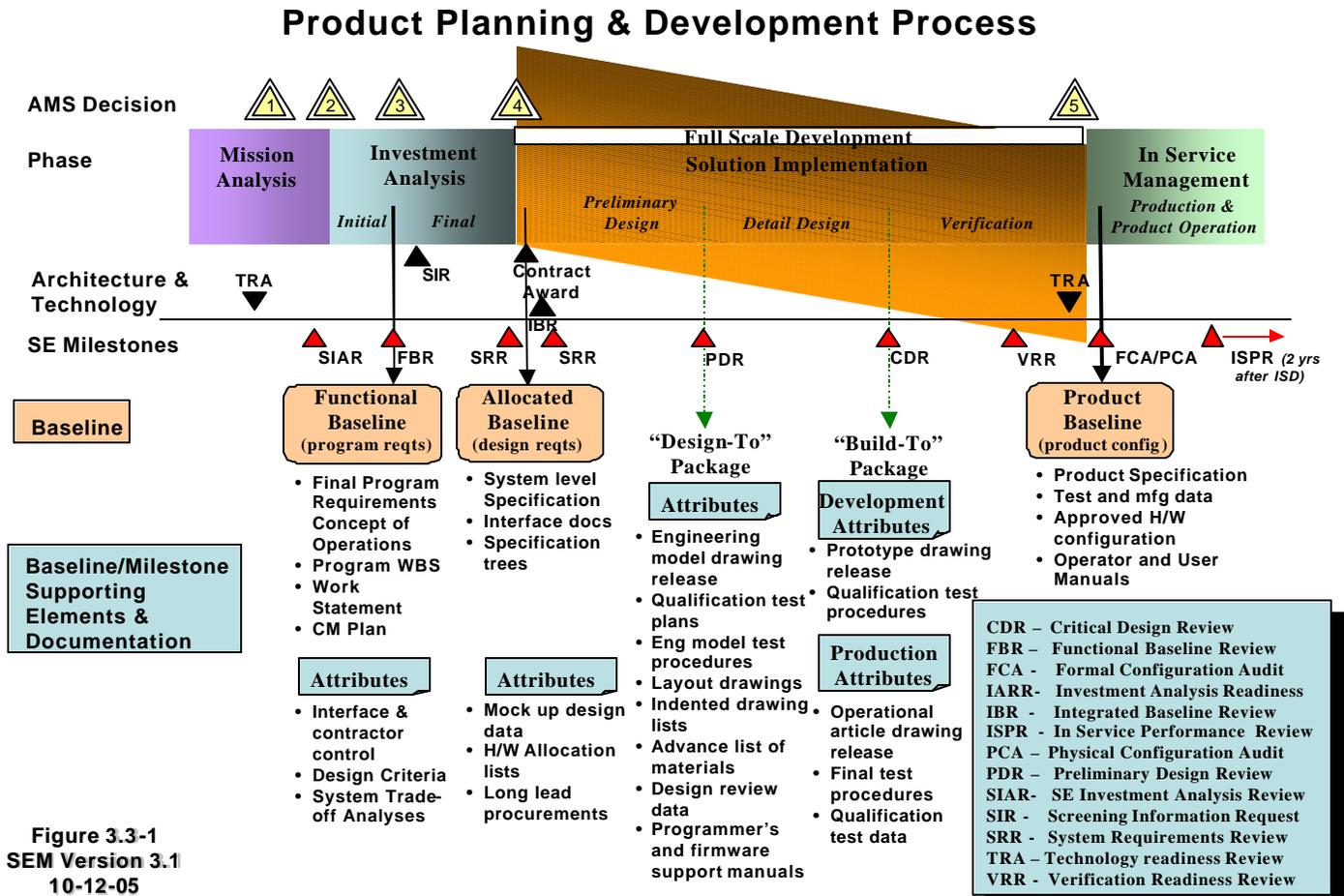


Figure 3.3-1  
 SEM Version 3.1  
 10-12-05

Figure 4.11-3. CM and Product Planning and Development Process

#### 4.11.3.2.2.1 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. The typical milestone, which must be met before this baseline is established, is successful completion of the functional baseline review. The functional baseline is managed through a formal control process using the change vehicle(s) documented in the developer’s approved CM plan and/or the customer’s formal change proposal form, if different (e.g., the NAS NCP form). The sponsor has final approval authority over changes to the functional baseline. The functional baseline for a NAS program is the final Program Requirements (fPR), attachment 1 to the Exhibit 300 documentation.

#### 4.11.3.2.2.1.1 NAS Functional Baseline

The technical portion of the NAS Enterprise Architecture defines and translates services, capabilities, and operational improvements into design solutions and their required technical characteristics. The technical characteristics are “NAS-Level Requirements” that explicitly translate the operational needs of the agency into functional, performance, and constraint requirements that are sufficient to direct the appropriate design and development of NAS systems. NAS-Level Requirements are the highest level requirements maintained within the FAA and are initially defined during Investment Analysis. The NAS functional baseline consists of two elements: the NAS-level requirements and Final Program Requirements (see FAA Order 1800.66, paragraph 3.3.3.1).

#### 4.11.3.2.2.2 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 just before contract award after the system requirements review. Generally, the allocated baseline is managed through a formal control process using the change vehicle(s) documented in the developer's approved CM plan and/or the customer's formal change proposal form. The allocated baseline for the FAA is the System Level Specification and Interface documentation that will be used for an acquisition program. Typically in the FAA, the contractor manages the allocated baseline; however, the FAA has final approval authority over changes.

#### 4.11.3.2.2.3 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 CI for production/procurement. This documentation package incorporates the allocated 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, as deemed necessary for CI acquisition.

The milestones for establishing this baseline are completion of the formal functional audit (FCA) and the physical configuration audit (PCA). The FCA is the formal review of final test documentation and test reports, users and operators manuals, and diagnostic manual; it is also required for conducting a PCA. The PCA is the formal examination of the "as-built" configuration of a CI against its technical documentation to establish or verify the CI's product baseline. In other words, the PCA compares the actual configuration of a production representative item against the final Type C product specification, referenced documentation, drawings, software product specification, and version description document used to produce that item. The product baseline is managed through a formal control process using the customer's change vehicle as documented in the customer's organizational CM policy and plan. To manage the product baseline, the FAA uses FAA form 1800-2, NCP; the program trouble report (PTR), which captures proposed corrective action for software; and the hardware discrepancy report (HDR), which captures proposed corrective action for hardware,

#### 4.11.3.2.2.4 Facility Baseline

The facility baseline is ***the information needed to identify and control changes as well as record configuration and change implementation status of all CIs under Regional CCB authority.*** There are two important categories of facility data subject to CM: facility baseline drawings and engineering data such as critical power panel schedules. Refer to FAA-STD-058, Federal Aviation Administration Standard Practice Facility Configuration Management, for specific criteria.

As discussed above, the FAA manages the NAS through the traditional functional, allocated, and product baselines. Additionally, the FAA manages the facility baseline. This baseline is an essential element of FAA planning for introducing NAS systems/subsystems. Facility baselines are a major component of the transition planning process, as described in FAA-STD-058. The complexities and variety of new projects to be implemented result in competition for floor and/or roof space, electrical power, and environmental and operational resources. Consequently, regional CMPs and CCB charters define space, power, and other resources as CIs that must be managed for each facility in the NAS.

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. When required, regional CM personnel request a change through the use of an NCP to establish or change the baseline (see FAA Order 1800.66, paragraph 3.3.3.5).

#### 4.11.3.2.2.5 Operational Baseline

The operational baseline is ***the approved technical documentation representing installed operational hardware and software.*** This represents the product baseline adapted to local conditions.

Operational baselines comprise the technical documentation that initially describes a delivered system and changes to it that occur as a result of in-service modifications and improvements or 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.

The process of establishing the operational baseline begins with approval of the product baseline NCP by the responsible CCB. The operational baseline documents listed in the approved NCP are entered into the NAS MCI as the technical representation of installed operational hardware and software. This set of documents shall accurately reflect each NAS subsystem at the beginning of its service life.

Because systems entering active service need to correct problems or provide enhancements, they will use the CM process. Although any organization may identify proposed changes, only the NCP process can be used to authorize a change. When a change is approved, all documents identified in the operational baseline shall reflect that change.

New documents, tools, or controls may be added to the operational baseline at any time. Examples of new operational baseline items include aids to creating firmware; engineering or documentation release processes; item marking associated with specific sites; or additional systemwide instructions such as maintenance handbooks. New operational baseline items are added by processing a change through the NCP process.

### 4.11.3.3 Step 3: Manage Approved Baseline Changes

Configuration control is ***the systematic process that ensures that baseline changes are properly identified, documented, evaluated, and approved by the appropriate level of authority and implemented and verified.*** A change is “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.”<sup>3</sup> Documented process requirements determine the level of control.

#### 4.11.3.3.1 Step 3.1: Identify and Describe Change

Changes to baselines are documented on the applicable change vehicles. In the FAA, any person can identify a problem or suggest an improvement at any time during the product lifecycle. 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 agreed-to CM planning documentation. Change vehicles state the problem or need for change, the proposed change, affected CI, cost and schedule for change implementation, and so forth. Change vehicles are uniquely identified and require the baseline elements (e.g., product identifier and document number) affected. For NAS baseline management, the FAA uses FAA form 1800-2, which represents proposed changes to the form, fit, or function (or Class I type change) of CIs identified as part of the NAS baseline. PTRs and HDRs are the vehicles used, primarily by operational support personnel, to correct a problem or inconsistency (or Class II type change) that does not impact any aspect of a baseline.

#### 4.11.3.3.2 Step 3.2: 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 (e.g., NAS baseline and work-product baseline changes).

#### 4.11.3.3.3 Step 3.3: 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 a forum for adjudicating changes for formal baselines.

In the FAA, the CCB structure has an established hierarchy. The NAS CCB is the highest ranking FAA board and has the authority to charter subordinate Solution Provider, Regional, and other CCBs, such as the William J. Hughes Technical Center CCB. The NAS CCB has general oversight responsibility for ensuring consistency across all CCBs. The NAS CCB also resolves issues elevated from subordinate CCBs. The NAS CCB charter and operating procedures detail the NAS CCB relationship and interaction with other chartered CCBs.

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, as listed in Appendix A of its charter as well as any other responsibilities specifically identified in the charter. These CCBs may approve any change as long as the CI is assigned to the CCB, and the appropriate source of funding is available when

---

<sup>3</sup> ANSI/EIA-649-1998, National Consensus Standard for Configuration Management.

cost impact is involved. When a source of funding is not identified, the CCB must follow agency procedures for obtaining the funds (see FAA Order 1800.66, paragraph 3.4.1).

#### **4.11.3.3.4 Step 3.4: Monitor Change Implementation**

An important CM function is monitoring change implementation. This activity ensures completion and release of approved changes.

Change implementation is accomplished by closure of the Configuration Control Decision (CCD). The CCD is the official FAA notification of CCB decisions and directives. The CCD identifies required actions and the organizations responsible for completing either implementation of approved changes or follow-up of actions for disapproved changes. CCD actions for approved changes may include physical incorporation of changes to affected hardware, software or facilities; approval of technical evaluations, studies, or tests; and directions for incorporating changes in baseline documentation. The primary activities of the CCD closure process for changes to facilities or operational equipment are field modification installation and tracking. The CCB monitors the actions listed in the CCD until all have been completed.

CCD closure consists of implementing defined actions, tracking completion of these actions, and ensuring their closeout in the appropriate information management systems (e.g., the Documentation Control Center and Maintenance Management System). CCD actions may include approval of physical incorporation of changes to affected hardware, software, or facilities; approval of technical evaluations, studies, or tests; and directions for incorporation of changes in baseline documentation. Field modification installation and tracking are the primary activities of the CCD closure process involving changes to facilities or operational equipment.

#### **4.11.3.4 Step 4: Provide Configuration Status Accounting (CSA)**

CSA is *the systematic recording and reporting of system or product configuration status*. CSA includes baseline change status and history for all items shown in the MCI, from initial delivery to the end of product service. CSA reports not only communicate status, but may also support conduct of formal configuration audits when design documentation is not available or has not been updated to the current configuration. CSA is performed at all levels of CM across a system or product lifecycle.

##### **4.11.3.4.1 Step 4.1: Capture Change Data**

Capturing change data, typically by using automated CM support tools, enables recording and reporting of the status and history of baseline changes from initiation through implementation.

##### **4.11.3.4.2 Step 4.2: Establish Baseline Configuration Status**

Once any of the baseline types is established, it can exist in two states: baseline and baseline with changes outstanding. When the outstanding changes are incorporated into the affected baseline, they become the updated baseline.

###### **4.11.3.4.2.1 Baseline**

Baselines that are established in Step 2.2, Baseline Establishment and Maintenance, are identified with a configuration identification nomenclature and the baseline approval date. For example, the original version of an FAA specification is identified as "FAA-E-2570, April 1, 1985."

#### 4.11.3.4.2.2 Baseline With Changes Outstanding

Baselines with changes outstanding that have been processed through Step 3, Manage Approved Baseline Changes result in a set of independent “Approved Baseline Changes” that will be applied to modify or extend the extant baseline. Until the approved baseline changes have been incorporated into the baseline, they are managed as independent CM products. A baseline with changes is identified as “the original baseline configuration identification nomenclature with change X” and the date the change was approved. For example, the original version of an FAA specification with changes is identified as “FAA-E-2570, April 1, 1985, **Change 1**, December 31, 1988.”



Updated baselines that have been processed through Step 3, Manage Approved Baseline Changes, become the new baseline when approved. Updated baselines are established by integrating all the outstanding approved baseline changes when their number becomes so numerous or a single change is so large that the baseline becomes unmanageable. The update sequence may be different than the approval sequence, with the net result that some parameter values may vary from the individual changes. The updated baseline is identified as the “original baseline configuration nomenclature with a revision identifier and the date the revised baseline was approved.” For example, an updated FAA specification is identified as “FAA-E-2570a, September 30, 1992.”

#### 4.11.3.5 Step 5: Verify and Audit Configuration

Conducting audits and quality checks ensures the integrity of the system or product. The FCA/PCA is a formal audit activity used to establish the product baseline and is discussed in Section 4.2.6 (Technical Reviews and Audits) of this manual. 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.

### 4.11.4 Outputs

#### 4.11.4.1 External

External outputs are information provided to the customer or receiving process that is outside the SE discipline processes. Major external outputs include the following.

- **Baselines and Updated Baselines.** The CM process provides the mechanism to establish and manage baselines. Baselines are established at completion of each CM milestone shown in Figure 4.11-3. Each baseline type is provided as a baseline or an updated baseline as described in subsection 4.11.3.4.
- **Baseline Changes.** Baseline changes are provided to all CM users whenever a potential baseline change or update is pending that could impact their work product.
- **Configuration Status Accounting Reports.** Configuration status accounting reports (CSAR) provide the current status of MCI configuration items or work products. CSARs can be generated electronically and provided on demand or at scheduled intervals by the supporting CM process.

#### 4.11.4.2 Internal

Internal outputs are information provided to the customer or receiving process that is within the SE discipline processes. Major internal outputs from CM are detailed below.

##### 4.11.4.2.1 Requirements Management

- **Baselines and Updated Baselines.** After approval by the responsible authority, requirements are to be incorporated into the appropriate baselines.
- **Baseline Changes.** Baseline changes are provided to all CM users whenever a potential baseline change or update is pending that could impact their work product.

##### 4.11.4.2.2 Synthesis

- **Baselines and Updated Baselines.** The Synthesis process uses baselines or baseline subsets to manage changes, promote visibility, and communicate status of the baseline or its components.
- **Baseline Changes.** Baseline changes are provided to all CM users whenever a potential baseline change or update is pending that could impact their work product.
- **Configuration Status Accounting Reports.** CSARs provide the current status of configuration items or work products. They can be generated electronically and provided on demand or at scheduled intervals by the supporting CM process.

##### 4.11.4.2.3 Risk Management

Program or system concerns and issues found during the CM process are outputs to the Risk Management process. These concerns and issues are typically found during review of changes or at the CCB meeting and require resolution outside of the CM process.

##### 4.11.4.2.4 Lifecycle Engineering

- **Baselines.** The Lifecycle Engineering process uses baselines to manage changes, promote visibility, and communicate status of the baseline or its components.
- **Baseline Changes.** Baseline changes are provided to all CM users whenever a potential baseline change or update is pending that could impact their work product.
- **Configuration Status Accounting Reports.** The CM process provides the Validation and Verification process with CSARs that communicate the status of the current baseline, including associated change history. CSARs are used specifically to document configuration status of specific products by effectivity and to document consistency between that specific item and its associated configuration documentation. This is done to establish that an adequate CM process is in place to provide control of the delivered configuration from the producer.

#### 4.11.4.2.5 Validation and Verification

- **Baselines.** The Validation and Verification process uses baselines to determine the extent that demonstration and test articles represent the baseline configuration.
- **Approved Baseline Changes.** Baseline changes are provided to all CM users whenever a potential baseline change or update is pending that could impact their work product.
- **Configuration Status Accounting Reports.** The CM process provides the Validation and Verification process with CSARs that communicate the status of the current baseline of delivered products, including associated change history. CSARs are used during verification activities to ensure that the modified product meets the documented requirements. CSARs are also used when design documentation is not available or has not been updated to the current configuration.

#### 4.11.4.2.6 Integrated Technical Planning

The CM process receives as input requests for information. Integrated Technical Planning receives CM planning criteria for such documents as the SEMP and supporting Technical Plans.

#### 4.11.4.2.7 Interface Management

- **Baselines and Updated Baselines.** The Interface Management process uses baselines or baseline subsets to manage changes to system interfaces, promote visibility, and communicate status of the baseline or its components.
- **Configuration Status Account Reports.** CSARs provide the current status of CIs or ICDs. They are generated electronically and provided upon demand or at scheduled intervals by the supporting CM process.

#### 4.11.4.2.8 Specialty Engineering

- **Baselines.** The Specialty Engineering process uses baselines to support analysis of proposed systems or associated components. The baseline is the basis for any changes, such as design features, operating maintenance, or installation procedures.
- **Baseline Changes.** Baseline changes are provided to all CM users whenever a potential baseline change or update is pending that could impact their work product.

#### 4.11.4.2.9 Integrity of Analyses

- **Baselines.** The Integrity of Analyses process uses baselines to support the appropriate application of the required level of fidelity, accuracy, and confirmed results of analyses that other SE processes perform.

- **Baseline Changes.** Baseline changes are provided to all CM users whenever a potential baseline change or update is pending that could impact their work product.

#### 4.11.5 Data Management

Data Management (DM) 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.*

##### 4.11.5.1 Control of Digital Data

DM includes controlling information in digital format to ensure integrity of digital representations of system or product information and other related data. DM shall include effective file and database management; unique identification of documents, files, and document representations; retention of essential file and version relationships; data status; and controlled access to digital data. Digital data is information prepared and maintained electronically and provided by electronic data access, interchange, transfer, or on electronic media. It should be noted that the control of digital data involves applying tailored requirements based on the CM practices (Figure 4.11.1) in this section.

The FAA has a number of policies regarding control of information, and this documentation should be referred to when planning for control of electronic data. If there is no applicable policy, refer to Section 5.6 of EIA 649 to develop criteria. There is, however, documented practice for managing work products within programs.

##### 4.11.5.2 Control of Work Products

In the context of managing NAS products or systems, work products are supporting products of the NAS, while not formally part of a NAS product's configuration. Work products developed within the program/project requiring management's signature must undergo CM. Work products associated with the program/project to undergo CM are identified, and requirements for controlling changes to those work products are established. CM of key work products identified should be applied consistently throughout the organization. Key work products are derived from the AMS and are determined by the project leader. Key work products encompass, but are not limited to, the required AMS documentation, including the Implementation Strategy and Planning document, requirements, contract documentation, CCB charters and operating procedures, plans, policies, procedures, and formal meeting minutes. As with any CM activity, work product procedures should be documented and included in planning documentation to ensure consistency and quality of work products.

###### 4.11.5.2.1 Identification of Work Products To Be Controlled

In accordance with agency or organizational policy or practices, each work product must be assigned a unique identifier and tracked using version or revision levels (including preliminary versions and drafts). File-naming conventions are to be consistent and easily traceable to the product title.

Electronic files are to be maintained to allow traceability to historical records of individual files. Each new version or revision of a file must have its own unique identifier. The original file will not be overwritten. See FAA Order 1800.66, paragraph 3.3.2.5 Data Management, for detailed procedures.



Suggested minimum formats for document working versions are the following: The original file would be named "FileName\_v1.0," and revisions would be named "FileName\_v1.1," "FileName\_v1.2," "Filename \_v1.3," and so forth.



Work product revisions requiring signature for formal release should begin, for example, at version 1.0 or revision 0 for the initial release of a document. The next revision for that document released for signature would be submitted as version 2.0 or revision A. Working review versions between major updates would be named versions 1.2, 1.3, 1.4, etc.

#### **4.11.5.2.2 Review of Work Products**

Formal review and version control of identified key work products are required to ensure accuracy, completeness, and traceability of changes. Key work products and associated change history are to be maintained in the program support library (PSL). Each person responsible for preparing a work product is to perform version control for that product.

#### **4.11.5.2.3 Perform Quality Checks**

Before being signed or released, key work products must be processed through quality assurance and/or peer review. Proof of quality assurance and/or peer review is to be maintained with the work product in the PSL.

#### **4.11.6 Configuration Metrics**

CM process metrics support evaluation of the effectiveness of a CM program and CM process improvement requirements. CM metrics criteria should be associated with each CM process task. The metrics support the program goals and provide good insight into process improvements.

Examples of effective CM metrics are:

- CM Plan development milestones
- Extent of adherence to the CM plan
- Number of changes processed, adopted, rejected, or open
- Status of open change requests
- Classification of change requests (i.e., Critical, Normal, Documentation, etc.)
- Number of deviations or waivers
- Cycle time for change processing
- Rate of baseline changes
- Time for CCD closure after approval
- Response time for comments on data manage documents

#### **4.11.7 References**

1. Blanchard, B. *System Engineering Management*. Second Edition. John Wiley & Sons, Inc., 1998.
2. *National Consensus Standard for Configuration Management*. EIA-649. Arlington, VA: Electronic Industries Alliance, August 1998.
3. *National Airspace System Configuration Management Policy*. FAA Order 1800.66. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, January 1999.
4. Samaras, Thomas. *Configuration Management Deskbook*. Advanced Applications Consultants, Inc., 1988.

## 4.12 Validation and Verification

Validation and Verification is the System Engineering (SE) process that confirms that system requirements are correct and satisfied (Figure 4.12-1). The Validation process confirms that the right system is being built (i.e., that the system requirements are unambiguous, correct, complete, consistent, operationally and technically feasible, and verifiable). The Verification process ensures that the design solution has met the system requirements and that the system is ready for use in the operational environment for which it is intended. This section describes the Validation and Verification process, including the inputs, outputs, and specific tasks of Validation and Verification.

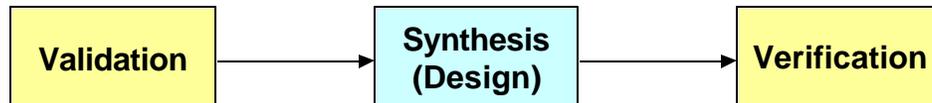


Figure 4.12-1. Validation and Verification's Role in System Development Process

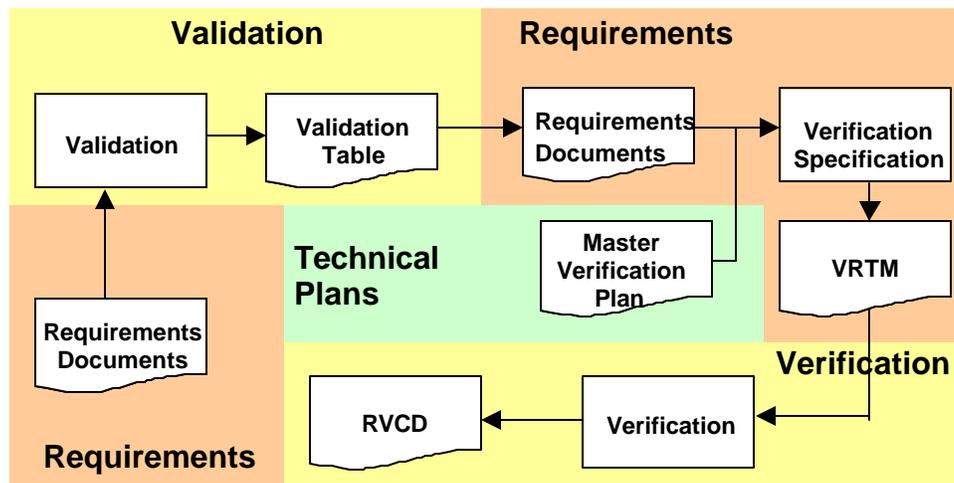


Figure 4.12-2. Validation and Verification Activities

The Validation and Verification activities, illustrated in Figure 4.12-2, are summarized below:

- Requirements feed Validation. During Validation activities, a Validation Table is developed that is included in a Validation Report when completed. The Validation Report is an input to the requirements document. The Validation Table becomes the basis for later Verification activities.
- At the same time, work begins on Verification planning and is documented in a “living” joint SE and Test and Evaluation (T&E) Master Verification Plan (MVP)(described and developed under Integrated Technical Planning (Section 4.2)).
- After Verification planning is completed, a specification/approach for verifying each requirement is developed in Requirements Management (Section 4.3) and documented for each requirement in the Validation Table. This update to the Validation Table transforms it into a Verification Requirements Traceability Matrix (VRTM), which becomes the foundation for the next activity and is included in the MVP as an update.

- After Verification activities are performed, the VRTM is updated with evidence of completion of activities. Using the updated VRTM, the Verification team develops the Requirements Verification Compliance Document (RVCD) to record completion of the Verification effort. The RVCD also identifies system compliance or noncompliance with the set of requirements used for the Verification activities. Program management uses this information for the Risk Management process (Section 4.10).

#### **4.12.1 Validation**

As stated earlier, the Validation process (Figure 4.12-3) confirms that the right system is being built (i.e., that the system requirements are unambiguous, correct, complete, consistent, operationally and technically feasible, and verifiable). The process is conducted in order to demonstrate that the requirements for a system are clearly understood and that it is possible to satisfy the requirements through design work using available state-of-the-art technology, funding, and schedule.

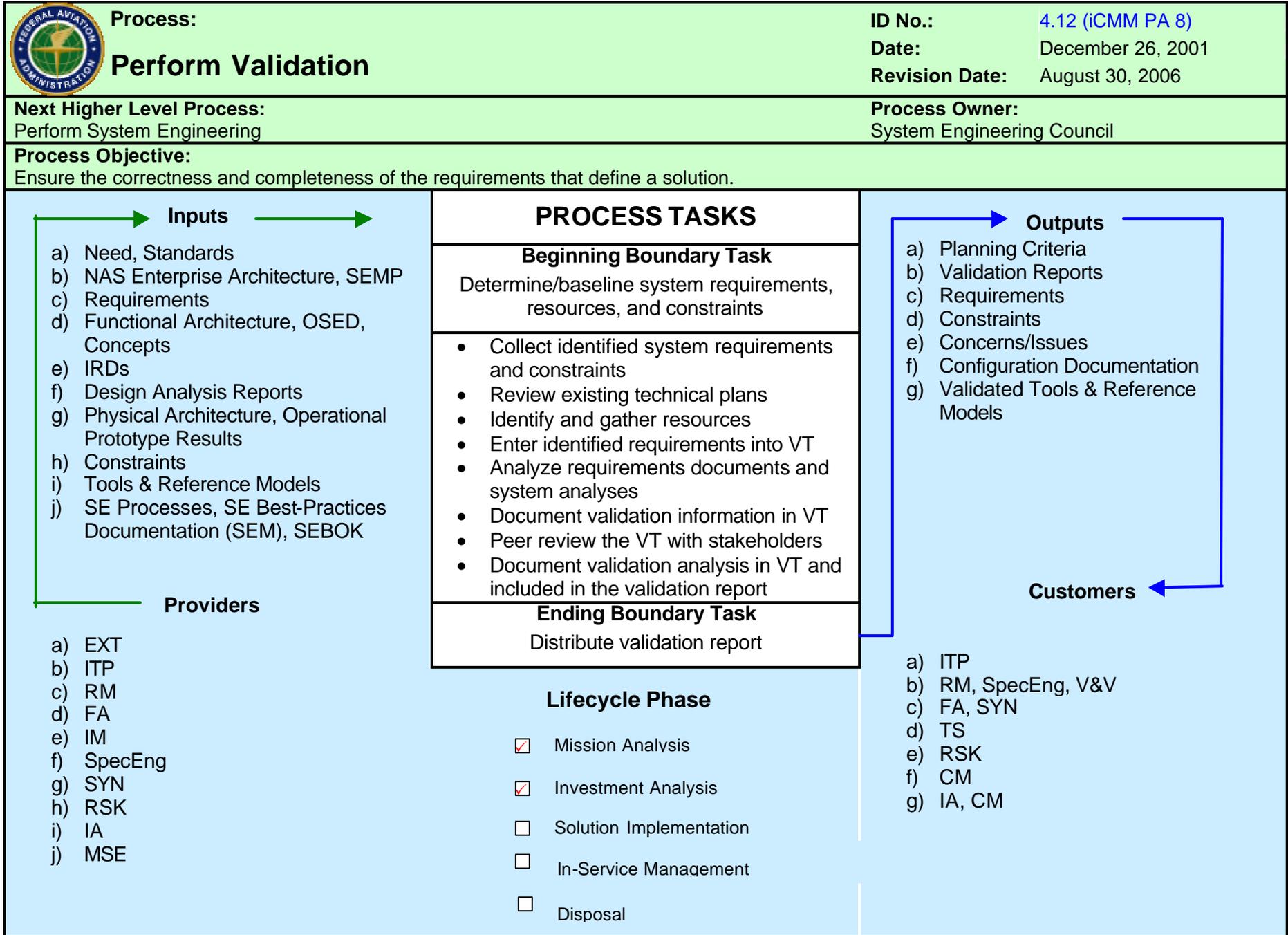


Figure 4.12-3. Validation Process-Based Management Chart

The Validation process is repeated incrementally at all stages of requirements development to ensure that the design at all levels is consistent with the intended mission. Validation follows the development of system requirements. Since these requirements are hierarchical in nature and developed in increasing detail as the lifecycle progresses, Validation is a staged process (Figure 4.12-4). Thus, as each level of requirements is developed, the requirements at that level undergo Validation, after which each validated requirement undergoes Verification.

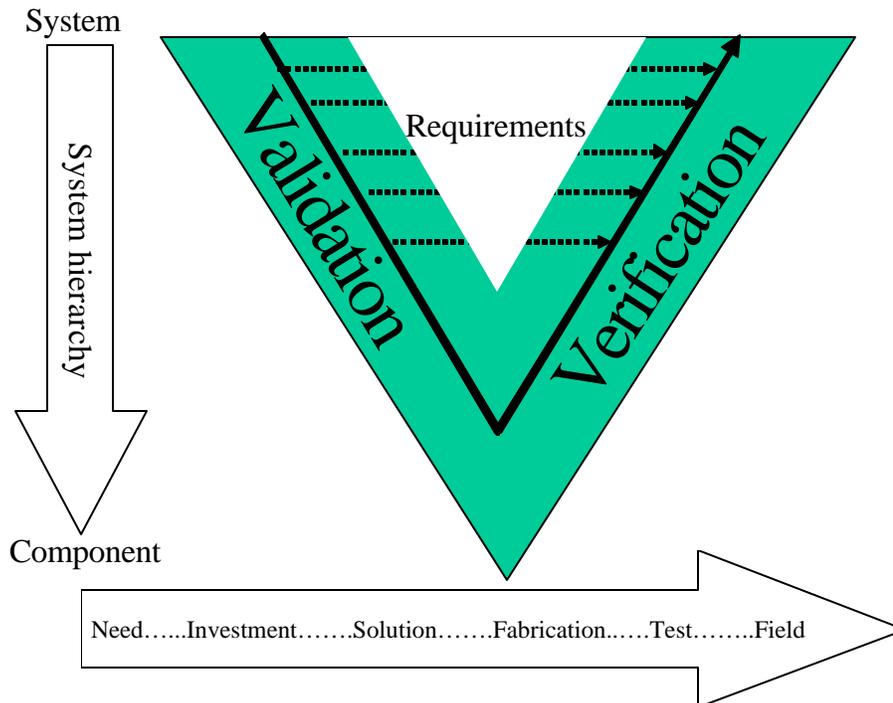


Figure 4.12-4. System Engineering "V" Diagram

A large part of this SE activity is challenging the need for the requirements need and the requirements' associated values before development of solutions. This activity helps to ensure that an economy of effort exists on the project and that resources are not wasted on developing solutions for unnecessary requirements. At each stage, the Validation process provides increasing confidence of the correctness and completeness of system requirements.

#### 4.12.1.1 Definition of Validation

There are multiple definitions of the Validation process, but, for the purposes of this manual and the Federal Aviation Administration (FAA), the accepted definition of the Validation process is:

*the determination that the requirements for a product are sufficiently correct and complete. (SAE ARP 4761, 1996)*

#### 4.12.1.2 Objective of Validation

The primary objective of the Validation process is to ensure that requirements are correct and complete. In addition, the Validation process ensures that requirements defined for a system

are consistent with the characteristics listed in Requirements Management (Section 4.3). Successful Validation confirms that the identified requirements are justified, relevant, and logically correct in terms of the customer’s needs and operating environment. In addition, the Validation process also ensures that the identified set of requirements is complete (i.e., containing all essential elements). To achieve Validation’s objective, Validation activities are performed as early as possible in the development phase after requirements are identified; thus, Validation follows requirements development and precedes design solution.

The Validation process is conducted to find and correct poor requirements, which stem from three sources:

- Ambiguous requirements statements
- Incorrect (including unnecessary) requirements statements
- Incomplete (or omitted) requirements statements

#### 4.12.1.3 Interfaces With Other System Engineering Processes

The SE elements that interface with the Validation process appear in Figure 4.12-5 and are described in “Inputs to Validation” (subsection 4.12.1.4).

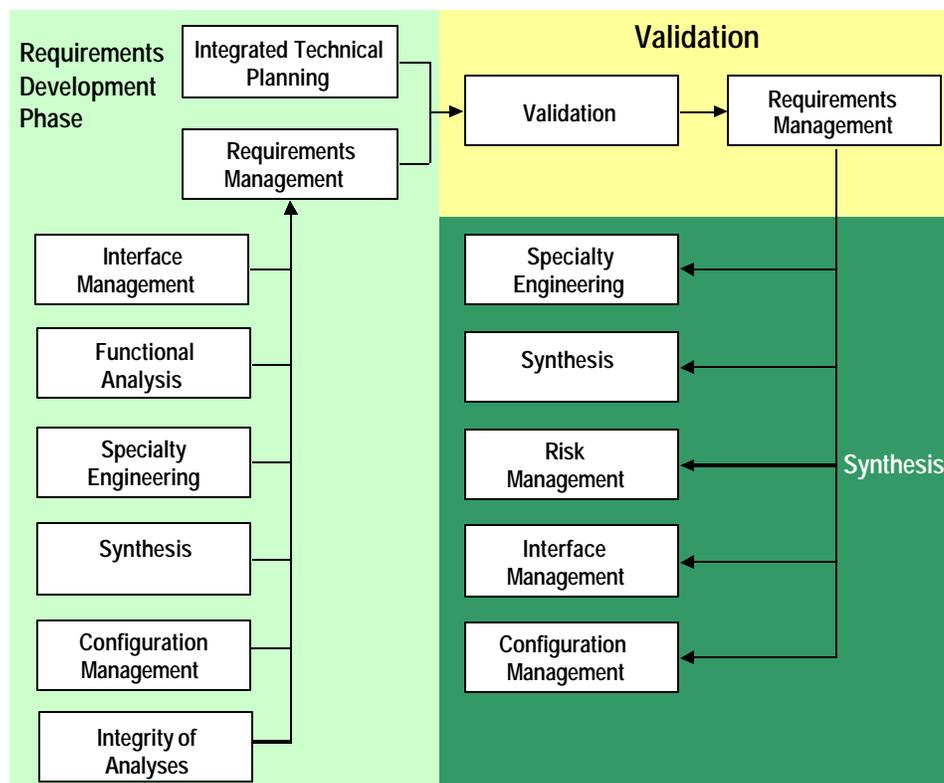


Figure 4.12-5. How Validation Interfaces with Other System Engineering Processes

#### 4.12.1.4 Inputs to Validation

The inputs to the Validation process include:

- stakeholder needs

- Standards
- Technical Plans (Integrated Program Plan (IPP), National Airspace System (NAS) Architecture, and program System Engineering Management Plan (SEMP))
- Requirements
- Functional Analysis (Functional Architecture, Operational Services and Environmental Description (OSED), and Concept of Operations (CONOPS))
- Operational Concept Demonstrations
- Interface Requirements Document(s) (IRD)
- Demonstrations
- Design Analysis Reports (DAR)
- NAS SEMP
- Physical Architecture

#### 4.12.1.4.1 Stakeholder needs

The original Stakeholder Need generated from a NAS stakeholder (or stakeholders) to identify a capability shortfall requires Validation. Once a Stakeholder Need is validated, SE continues to ultimately provide a balanced solution to the need.

#### 4.12.1.4.2 Standards

Industry and government standards are additional inputs to the Validation process. These documents often contain information required to validate the Requirements of a system not found in higher level requirements documents. They include publications and standards from the Society of Automotive Engineers (SAE), the International Organization of Standards (ISO), and the Electronics Industry Alliance (EIA), as well as U.S. Government advisory circulars and FAA regulations.

#### 4.12.1.4.3 Technical Plans

Technical plans are an output of the Integrated Technical Planning process (Section 4.2). These plans define the program's tailored tasks for conducting Validation and Verification for a specific program. The IPP lays out the overall program and details the program's planned activities. The FAA Acquisition System Toolset (FAST) (<http://fast.faa.gov/ams/ippdesc.htm>) supplies a complete description of the IPP, and Integrated Technical Planning discusses SE's role in producing the IPP. In addition to the IPP, the program's SEMP and the NAS Architecture shall be used as inputs to the Validation process. The NAS Architecture is considered a part of the technical plans package in that it defines the FAA framework for future systems in the NAS. This architecture is a useful resource for validating the Requirements for systems developed for NAS modernization.

#### 4.12.1.4.4 Requirements

Requirements documents are outputs from the Requirements Management process (Section 4.3). These documents include the initial Requirements Document (iRD) and final

Requirements Documents (fRD) (as they become available), as well as supporting documents such as:

- Program and technical requirements
- Customer operational requirements, including the Mission Need Statement (MNS)
- Regulatory, agency, and statutory requirements

The Requirements are classified under several categories described in “Requirements Category” (subsection 4.3.3.2.1.4.3). The two major categories are (1) program requirements and (2) technical requirements. Program requirements are imposed on vendors through contracts, not specifications. Technical requirements apply to the system or service under acquisition, and they are described in requirements documents, system specifications, and IRDs.

#### **4.12.1.4.5 Functional Analysis**

The Functional Analysis process (Section 4.4) is an SE tool that provides a functional (what the system does, not how) description of a system that becomes a framework for synthesis and requirements development. It is recommended that the output of this process be used to validate Requirements. The outputs of this process are:

- Functional Architecture(s)
- OSED (RTCA/DO-264, Appendix C, System Safety Handbook (SSH), Sections 4.1.1 and 3.8)
- CONOPS

#### **4.12.1.4.6 Operational Concept Demonstrations**

Operational Concept Demonstrations (“Demonstrations” (subsection 4.8.0.4.8)) are conducted to determine and validate high-risk Requirements associated with an unvalidated CONOPS.

#### **4.12.1.4.7 Interface Requirements Documents**

IRDs are another example of system design information. These documents, which are outputs of the Interface Management process (Section 4.7), provide a deeper understanding of the underlying interfaces, functions, and reasons for the Requirements. These descriptions include the system-level interface definitions. Part of the Validation of a system is the assurance that the Requirements for these interfaces are correct.

#### **4.12.1.4.8 Demonstrations**

Specialty engineers, as deemed necessary, often conduct Demonstrations (“Demonstrations” (subsection 4.8.0.4.8)) as part of analysis efforts (e.g., maintainability demonstration or human factors demonstrations). These Demonstrations provide useful feedback on the effectiveness and value of various design alternatives. Additionally, the Demonstrations may generate information for use while Requirements are being validated.

#### 4.12.1.4.9 Design Analysis Reports

DARs are outputs of the Specialty Engineering process (Section 4.8). These reports document the results of the Specialty Engineering analyses, which may contribute to the identification, Validation, and Verification of Requirements.

#### 4.12.1.4.10 National Airspace System System Engineering Management Plan

The NAS SEMP defines the overall plan for SE in the Acquisition Management System (AMS). This plan details *who*, *what*, *when*, and *why* SE tasks are performed in support of AMS programs. The System Engineering Manual (SEM), on the other hand, defines how the SE processes are performed.

#### 4.12.1.4.11 Physical Architecture

The Physical Architecture is essentially the engineering design of the system that is produced via the Synthesis process (Section 4.5). This information may vary in detail, depending on the phase of the program. This input is essential so that the persons responsible for the Validation process understand the product Requirements and configuration (if available). Information includes:

- Drawings (if updating current systems and if they exist in the Validation phase)
- Design descriptions
- System descriptions

#### 4.12.1.5 The Validation Process

The following sections describe the purpose, general outcomes/expectations, and tasks of the Validation process.

##### 4.12.1.5.1 Validation Process Purpose

Validation is primarily performed to ensure the correctness and completeness of the requirements that define a system. Aerospace Recommended Procedure (ARP) 4754, Paragraph 7.1, defines correctness and completeness as follows:

- Correctness of a requirements statement means the absence of ambiguity or error in its attributes
- Completeness of a requirements statement means that no attributes have been omitted and that those stated are essential

System requirements are analyzed to ensure that the defined set of Requirements is consistent with the operational need defined in the CONOPS, Specialty Engineering analyses, and MNS. The Validation process is conducted to provide objective evidence that the services provided by the system, as defined in the requirements document, comply with the stakeholder needs, as defined in the analyses, CONOPS, and MNS. When variances are identified, they are recorded and used to guide corrective actions. Because Validation is a comparative assessment of Requirements against needs, it also results in confirmation that stakeholder needs are correctly identified and requested. Stakeholders normally ratify Validation of Requirements at the system level.

“Task 5: Analyze Requirements Documents and System Analyses” (subsection 4.12.1.5.3.5) describes the desired attributes of Requirements. The Requirements Management (Section 4.3) also describes the desired attributes of individual Requirements.

#### 4.12.1.5.2 Validation Process Objectives

The general objectives of the Validation process include:

- Development of the Validation Table and inclusion of the Validation Table in a Validation Report
- Appending to or referencing by the existing requirements documents of the Validation Report
- Confirmation that the system services required by stakeholders are properly documented in the Requirements
- Confirmation that the stakeholder requirements faithfully describe the required system services
- Reporting of nonconformance, which is used to guide corrective actions
- Traceability of all requirements to higher level Requirements
- Documentation of the program's concerns and issues and constraints

#### 4.12.1.5.3 Validation Process Tasks

All Requirements in all categories are required to be validated. In general, the Validation of higher level Requirements serves as a basis of Validation for lower level Requirements. The tasks involved in the Validation process are conducted in three phases: planning, evaluation, and documentation. The recommended process tasks for validating Requirements appear in Figure 4.12-3 (above) and Figure 4.12-6 and are described in the following subsections.

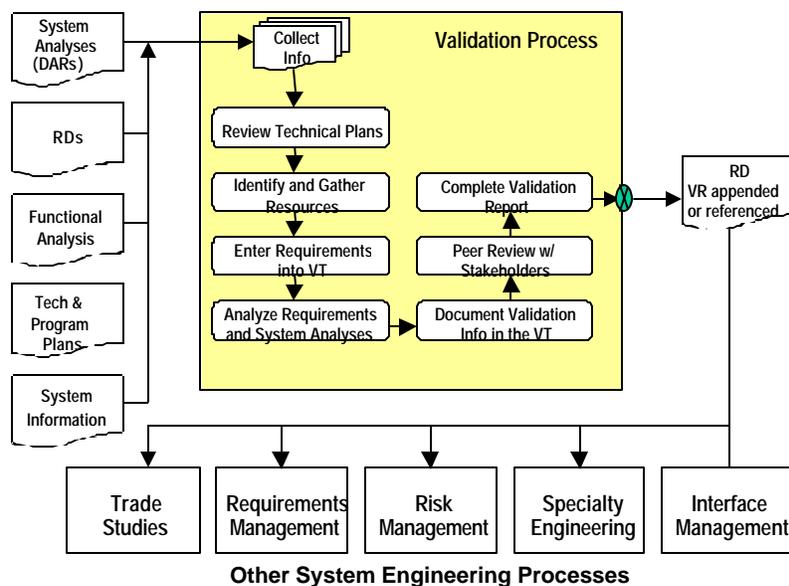


Figure 4.12-6. Overall Validation Process and Outputs

#### 4.12.1.5.3.1 Task 1: Collect Identified System Requirements and Constraints

The initial step in the Validation process is to accept the set of Requirements to be validated from the Requirements Management process (Section 4.3). In addition, the information required for Validation is gathered, which documents the baseline system requirements, resources, and constraints. These documents are described in “Inputs to Validation” (subsection 4.12.1.4 above) and include the requirements documents, technical plans, and system description information.

#### 4.12.1.5.3.2 Task 2: Review Existing Technical Plans

The next step is to review the program and acquisition plans, such as the IPP and the MVP, if it exists. These plans include the Validation tasks to be performed; allocation of responsibility to organizations; schedule; and costs. The objective is to define the strategy for validating the system’s services in its operational environment and achieving customer satisfaction in accordance with these plans. This strategy depends on the lifecycle stage (e.g., whether a model, prototype, or actual product is being verified); on risks (e.g., safety, technical, and commercial criticality issues); and on the agreement and organizational constraints of the stakeholder requirements. It is required that, where appropriate, Validation steps (e.g., various operational states, scenarios, and missions) be defined that progressively build confidence in compliance of the installed system and assist diagnosis of any noncompliance.

#### NOTE

*Where stakeholder needs are unable to be specified in advance or change frequently, repeated Validation of (often rapidly developed) increments in system evolution may be employed to refine stakeholder requirements and mitigate risks in the correct identification of need. For example, ISO 13407 describes an iterative lifecycle that involves users.*

#### 4.12.1.5.3.3 Task 3: Identify and Gather Resources

At this stage, the Validation resources are formed from the appropriate SE resources. These resources include tools, information, and organizations, including the execution teams, stakeholders, and SE.

#### 4.12.1.5.3.4 Task 4: Enter Identified Requirements Into Validation Table

This step involves entering or copying the Requirements from the requirements document into a table, spreadsheet, database, or other SE tool appropriate to managing the Validation of Requirements. Table 4.12-1 is an example of a typical Validation Table. Each Requirement and specification that defines a system, at all levels, shall be listed in a Validation Table.

Table 4.12-1. Example Validation Table

(PUI)	Requirement	Requirements Document or specification?	Validated? Y/N	Source(s)	Location in Source	Conformance information	Corrective Action Owner
Program Unique Identifier. Enter a unique number here to ID the Requirement. This ID is the paragraph number from the requirements document.	Copy the Requirement here verbatim from the requirements document and specification.	Identify where the Requirement is found.	Indicate whether the Requirement was validated.	Explain the source of the Validation, (e.g., a safety analysis or other means).	Where specifically in the source the Requirement is validated.	State conformance basis. If nonconformance is found, state recommended or required corrective action.	Organization or individual that owns the conformance or corrective action
3.2.1.1.1	The ADS-B system shall continue to operate normally in icing conditions up to heavy icing, as defined in 14 CFR FAR 25. (example only)	iRD	YES or check	IRD, ADS-B, OSA	IRD: Paragraph 3.2.1.1.1  OSA: Paragraph 2.5.5	System safety confirms that icing is expected in the operational environment description.	En Route Service

#### 4.12.1.5.3.5 Task 5: Analyze Requirements Documents and System Analyses

During Task 5, a review of the existing requirements documents is performed. Also during this task, the set of Requirements that is being evaluated for validity is compared to the existing higher level requirements documents. The Validation of higher level Requirements may serve as the basis for Validation of lower level Requirements, if traceability is demonstrable. If the existence of a validated Requirement in a higher level requirements document is shown, then lower-level Requirements that are traced from the validated Requirement may be partially validated on this basis. The lower level Requirements still need to meet the characteristics listed in “Validation Process Purpose” (subsection 4.12.1.5.1 above). For example, assume that a Requirement is listed in a validated MNS and the current task is to validate the functional requirements. If the functional requirement is traceable to a functional architecture based on the MNS (higher level), then the functional requirement (lower level) is considered partially validated by virtue of this traceability. However, the functional requirement in this example still requires evaluation of the characteristics listed in “Validation Process Purpose.” Once complete, the Requirement is considered validated.

If a Requirement is not contained in a higher level requirements document, then it is evaluated by detailed review of Functional Analyses, results of prototype evaluations, Specialty

Engineering analyses in documented DARs, specified design guides, CONOPS, the NAS Architecture, and other industry and government standards that describe the system and assess the system's needs and capability shortfalls. These documents often contain information needed to validate Requirements not found in higher level requirements documents. In these documents, the Verification team looks for candidate requirements, recommendations, functional requirements, and other information that confirm the need for the stated Requirement.

The following Validation principles shall be employed when performing Validation activities:

- Ensure that stakeholders and testers are an integral part of the Validation process
- Perform research and analysis to find information and/or related Requirements that confirm the need for a particular Requirement (e.g., a set of related Requirements may confirm the need and validity of a derived Requirement)
- Note Requirements that are unable to be confirmed; these Requirements are noted as nonconforming<sup>1</sup> and evaluated for removal in the Requirements Management process (Section 4.3)
- Conduct Validation activities to detect (in the system or services) the existence of random and systematic nonconformance to stakeholder requirements
- Ensure that the Validation process is undertaken in a manner consistent with defined and documented organizational practices to minimize uncertainty in the replication of Validation actions, conditions, and outcomes
- Maintain objective and authenticated records of Validation actions and outcomes
- Conduct fault resolution of a nonconformance in the Requirements Management process to a level of resolution consistent with cost-effective remedial action, including revalidating following defect correction and/or organizational quality improvement actions
- Conduct Validation activities to determine the correctness and completeness of the Requirements

When Validation is performed, the following correctness and completeness checks (may be tailored by expansion) shall be completed at each level of the Requirements hierarchy:

### **Correctness**

1. Requirements correctly stated:
  - What is required (design independent)
  - Unambiguous
  - Statements lead to appropriate design
  - Achievable with current or emerging technology

---

<sup>1</sup> Nonconformance means that a needed Requirement is missing or an existing Requirement is unable to be validated. In accordance with agreement terms or organizational objectives, Validation is conducted to isolate the part of the system that gives rise to a nonconformance, which may result in the need for corrective action and/or changes in quality management policy. "Objective of Validation" (subsection 4.12.1.2) discusses the sources of nonconformance.

- Requirement is verifiable
  - Stated for appropriate environmental conditions (ambient and operational)
  - Stated for normal and abnormal operations
  - Derived Requirements supported by analyses
  - Each Requirement has an identified source
2. Requirements correctly reflect the analyses:
- Appropriate analyses completed correctly
  - System hazards correctly identified and classified according to risk
  - System characteristics in DARs correctly identified and classified
  - Reliability, availability, fault detection, and tolerances identified
3. Functions correctly identified:
- Requirements based on functions
  - Functions significant to Requirements
  - Documented
  - Traced to higher functions
  - Constrained by higher level Requirements

### **Completeness**

1. Requirements traceable to an identified source:
- Functional Analysis
  - Higher level requirements documents
  - Safety assessments
  - Reliability, Maintainability, and Availability (RMA) analyses (Failure Modes and Effects Analysis (FMEA), Failure Modes and Effects Criticality Analysis (FMECA))
  - Requirements identified in DARs (Specialty Engineering (subsection 4.12.2.3.4 below))
  - Derived Requirements
  - Regulations, standards, or statutory requirements
  - OSED
  - Integration requirements
2. Constraints defined, substantiated, and addressed:
- State of the art
  - Safety
  - Environment

- Industry and FAA standards
  - Specify system implementation
  - Legacy systems
3. System implementation specified:
    - Functional Analysis completed
    - Requirements allocated to systems
    - Architecture defined at each functional level
    - Interfaces (internal and external) defined—human, hardware, software, physical, functional, procedural, and environmental (ambient and operational)
  4. All prohibited behaviors and characteristics explicitly stated
  5. All technical performance measures explicitly stated

#### **4.12.1.5.3.6 Task 6: Document Validation Information in Validation Table**

During this task, Validation data is collected, classified, and collated in the Validation Table described in “Task 4: Enter the Identified Requirements Into a Validation Table” (subsection 4.12.1.5.3.4 above) and in accordance with criteria defined in the program and acquisition plans. This process categorizes conforming and nonconforming Requirements according to their source and corrective action owner. The Validation data is then analyzed to detect essential features, such as trends and patterns of failure, evidence of systemic failings, and emerging threats to system services.

#### **4.12.1.5.3.7 Task 7: Peer Review Validation Table With Stakeholders**

During this task, the stakeholders of the system’s Requirements are identified. Once the Validation Table is filled, the stakeholders review it. Stakeholder comments are incorporated into the table, and the table is finalized.

#### **4.12.1.5.3.8 Task 8: Document Requirements Validation Analysis in Validation Table and Include Validation Table in Validation Report**

The results of the Validation analysis are documented in the Validation Table, and the Validation Table is included in a Validation Report. The Validation Report is transmitted to Requirements Management (Section 4.3). This report is appended to or referenced by the requirements document.

The Validation Report summarizes the Validation effort and results and communicates the Validation Table to other SE processes. The following format should be used as a guide for the contents and organization of a Validation Report.

Validation Report format:

- I. Summary of Validation efforts and results
  - a. Summarize the Validation results when locating conforming and nonconforming Requirements

- II. System and program description
- III. Methodology used
- IV. Unvalidated Requirements
  - a. List of nonconforming Requirements
  - b. Recommendations for correction of nonconforming Requirements
- V. Validation Table
- VI. Discussion of trends and patterns of failure, evidence of systemic failings, and emerging threats to system services

#### **4.12.1.6 Tailoring of Validation Activities**

Tailoring of a program's Validation activities is limited to the following:

- The specific means of Validation may include the techniques and tools employed and described in SAE ARP 4754, Section 7.7, if desired by the program
- The specific contents of the Validation Report may be tailored to include additional information as specified in "Task 8: Document the Requirements Validation Analysis in Validation Table and Include Validation Table in Validation Report" (subsection 4.12.1.5.3.8 above)

#### **4.12.2 Verification**

The Verification process ensures that the design solution has met the system requirements and that the system is ready for use in the operational environment for which it is intended. This description means that a verified system is able to demonstrate (show evidence) that it complies with mission need; functional, performance, allocated, derived, and interface requirements; and design and allocated constraints that achieve stakeholder needs. The Verification process (Figure 4.12-4 (above) and Figure 4.12-7) supports system evolution at all levels of the system's lifecycle, from concept to advanced studies and preliminary analyses to design and development, culminating in the production, product acceptance, operational, and disposal phases.

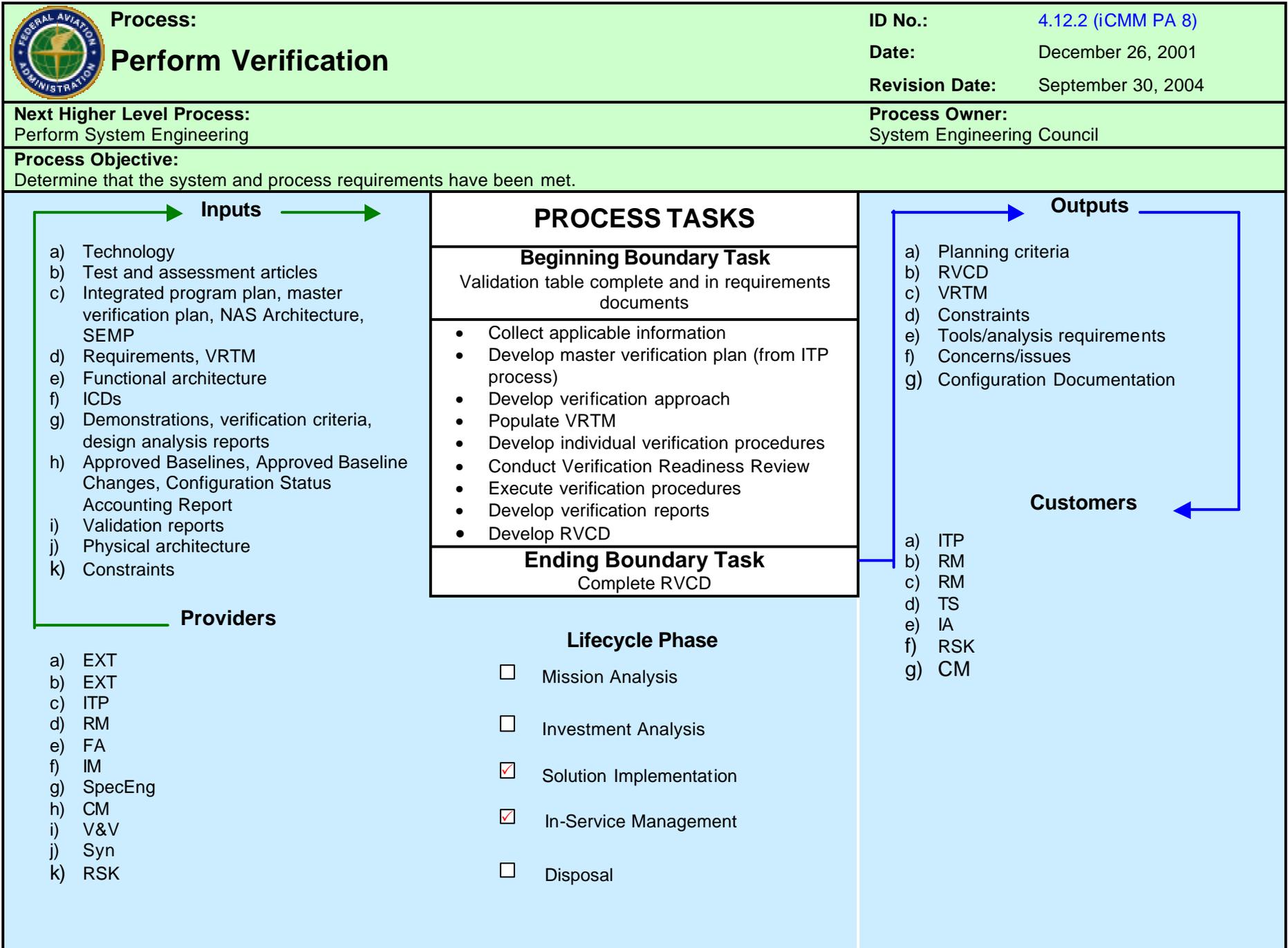


Figure 4.12-7. Verification Process-Based Management Chart

#### 4.12.2.1 Objectives of Verification

The major objectives of the Verification process are to confirm that:

- Intended functions are correctly implemented and that the system is operationally ready and acceptable to the users
- Requirements are satisfied
- Specialty Engineering analyses, including lifecycle, remain valid for the system as implemented

Successful Verification confirms that the development process has provided a system consistent with stakeholder needs and compliant with the system's validated requirements. It is a basic principle to verify all requirements in the system's requirements documents. This principle does not imply that a test is required for every requirement, but it does imply the need to conduct some form of Test and Evaluation (T&E) and/or SE Assessment at an appropriate level to ensure that all requirements are satisfied.

The broad range of product development cycles and levels of product development complexity require that the Verification process be tailored to each project.

The expected outcomes of Verification are development of:

- MVP (from the Integrated Technical Planning process (Section 4.2))
- VRTM
- Individual T&E and SE Assessment plans
- T&E procedures
- Verification Readiness Reviews (if applicable)
- T&E and SE Assessment reports, which detail specific test results and assessments
- RVCD, which provides documentation that the system product conforms to system requirements and includes nonconformance reports

#### 4.12.2.2 Definition of Verification

The accepted definition of verification for this manual and the FAA is:

*the evaluation of an implementation [system] to determine that applicable requirements are met. (SAE ARP 4761, 1996)*

Verification is the composite of all tasks, actions, and activities performed on system elements that are required to evaluate the progress and measure the effectiveness of evolving system products and processes in meeting system requirements. There are two basic and complementary methods of Verification: T&E and SE Assessment, as shown in Figure 4.12-8.

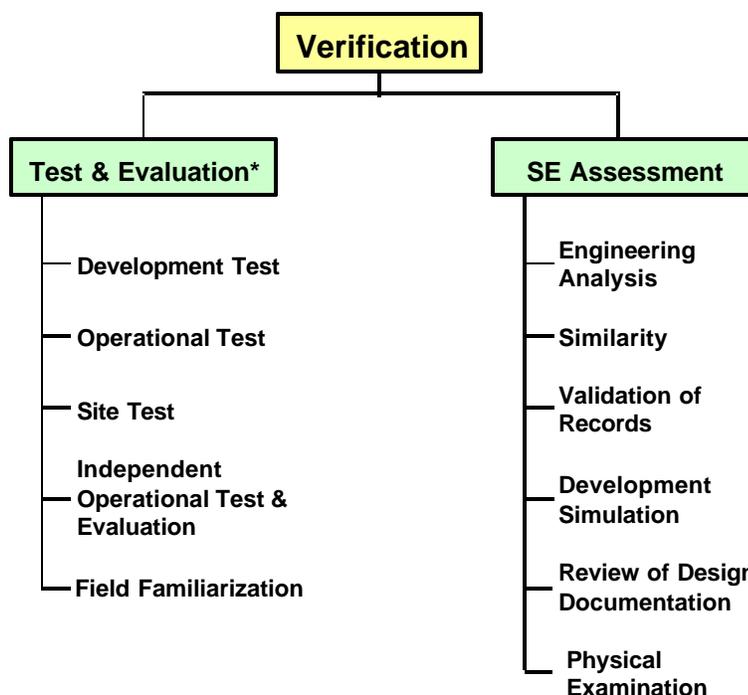
##### 4.12.2.2.1 Test and Evaluation Verification

It is recommended that T&E programs be structured to:

- Provide essential information to support decision making

- Provide essential information to assess technical and acquisition risk
- Verify attainment of technical performance specifications and objectives
- Verify that a system is operationally effective and suitable for its intended use

It is also recommended that T&E objectives for each AMS lifecycle phase be designed to mitigate potential operational risks and to demonstrate system performance appropriate to that phase. Quantitative criteria provide substantive evidence for analysis of hardware, software, and system maturity and readiness to proceed through the acquisition management process.



\* For more information, refer to the Test and Evaluation Process Guidelines Document on the FAA AMS Toolset (<http://fast.faa.gov>).

Figure 4.12-8. Components of Verification

It is recommended that each T&E phase have specific milestones (entrance and exit criteria) that are satisfied before the next T&E phase is entered. Parallel testing is encouraged when it is more efficient and at least as effective as serial testing.

It is highly desirable that system performance be established by test under actual (or simulated) operating conditions; however, these conditions may not be possible until the system is deployed. Problems uncovered at deployment are costly to correct; therefore, a combination of inspection, analysis, and test often is employed during program development to detect problems early, thereby reducing risk and helping to ensure a successful, cost-effective program.

Compliance with each requirement in a specification shall be verified by one or more of the methods described in this manual and as indicated in the VRTM.

T&E methods include:

- **Verification by Demonstration.** This method includes Verification accomplished by operation, adjustment, or reconfiguration of items performing their design functions under specific scenarios. The items may be instrumented and quantitative limits of performance monitored; however, only check sheets are required rather than recordings of actual performance data. This method is used when actual demonstration techniques may be used to verify compliance with a requirement. Observations made by engineers or instrumentation are compared with predetermined responses based on the requirements. An example of this Verification method is the demonstration of installing and uninstalling an aircraft engine in a specified amount of time. Demonstration is often used to verify compliance with requirements in servicing, reliability, maintainability, transportability, and human factors engineering.
- **Verification by Test.** This method is accomplished through systematic exercising of the application item under appropriate conditions, with or without instrumentation, and the collection, analysis, and evaluation of quantitative data.
- **Verification by Analysis.** This method is accomplished by technical or mathematical evaluation, mathematical models or simulation, algorithms, charts, circuit diagrams, and representative data.
- **Verification by Inspection.** This method is 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. Inspection is generally nondestructive and uses the senses of sight, hearing, smell, touch, and taste; simple physical manipulation; mechanical and electrical gauging and measurement; and other means of investigation. Inspection often verifies the physical design features of a system as well as construction features, workmanship, dimensions, quality, and physical conditions, such as cleanliness, installation, and finishing. Inspection may include reviews of documentation, system descriptions, and other materials to compare the actual system with predetermined standards.

The Test and Evaluation section of the FAST (<http://fast.faa.gov/toolsets/index.htm>) provides specific guidelines to conduct T&E.

#### 4.12.2.2 Verification by System Engineering Assessment

It is recommended that Verification by SE Assessment be conducted to support the development of products, services, and processes necessary to verify that system end-items satisfy their requirements. Verification assessment addresses Verification requirements and criteria for solution alternatives; definition of Verifications to demonstrate proof of concept; and development, qualification, acceptance, pertinent operational, and other testing. The assessment may also consider the requirements and procedures needed to verify critical Verification methods and processes (e.g., Verification of key methods and assumptions and the data used in Verification by analysis).

It is suggested that Verification assessment be initiated when a design concept is established. The Verification assessment is drawn from the MVP and the results of the Validation effort. According to the Integrated Technical Planning process (Section 4.2), the objective of the MVP is to define all Verification activities that demonstrate the system's capability to meet the requirements of its specification. These activities shall be fully integrated to ensure that adequate data is provided at minimum cost within the allotted timeframe. A continuing feedback

of Verification data throughout product development, test, and evaluation is necessary to reduce risk and to detect problems early. The goal is to completely verify the system's capability to meet all requirements before production and operational use.

SE Assessment methods include:

- **Verification by Engineering Analysis.** This process includes the techniques of SE analysis, Specialty Engineering, statistic and qualitative analysis, simulations, and modeling. Engineering analysis is used when testing is not feasible, similarity is nonapplicable, and inspection is inadequate.
- **Verification by Similarity.** This process assesses compliance with requirements by reviewing a similar system's test data, configuration, and applications. This method is only used when the systems are similar in design and manufacturing, and the prior system was qualified to equivalent or greater specifications. Great care is taken to ensure that the intended application environment of the emerging system is identical or less rigorous than the environment of the previous system testing.
- **Validation of Records.** This process reviews manufacturing records at end-item acceptance to verify features and requirements of the system.
- **Simulation.** This process verifies design features, system behavior, and performance using simulated models of the system.
- **Review of Design Documentation.** This process uses the disciplined review of design documentation, such as reports and drawings from Acquisition Reviews, Design Reviews (preliminary and critical), and other evaluations.
- **Physical Examination.** This process assesses compliance with requirements by visually inspecting a physical item or configuration according to preestablished criteria.

#### 4.12.2.3 Interfaces With Other System Engineering Processes

Verification has multiple interfaces with other SE elements. These interfaces are shown in Figure 4.12-9 and described in the following paragraphs.

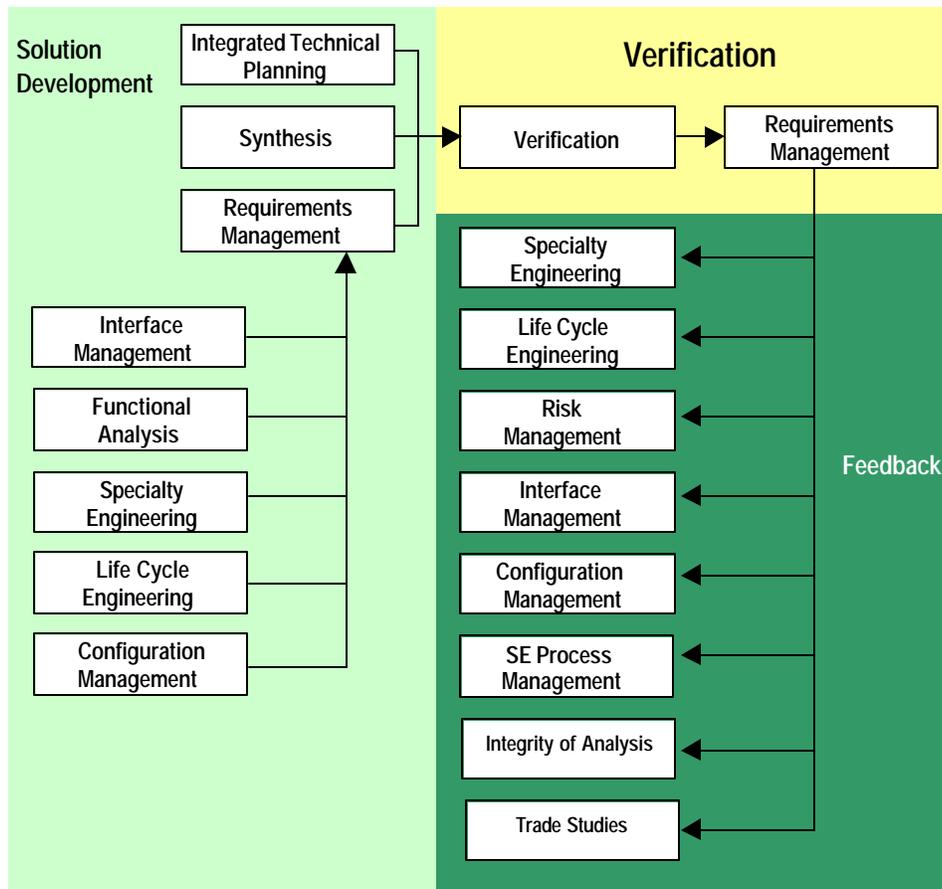


Figure 4.12-9. Verification Interfaces With Other System Engineering Elements

#### 4.12.2.3.1 Requirements Management

Requirements documents are outputs from the Requirements Management process (Section 4.3). These documents include the iRD and fRD, as well as underlying documents, such as customer operational requirements; system and technical requirements; and regulatory, agency, and statutory requirements. These documents also include the MNS and any Verification specification documents. The execution teams manage these documents.

#### 4.12.2.3.2 Synthesis

System, subsystem, component, and procedural designs comprise the outputs of the Synthesis process (Section 4.5). The information contained in these designs and, in some cases, test articles and/or prototypes is required for Verification.

#### 4.12.2.3.3 Integrated Technical Planning

Technical plans are an output of the Integrated Technical Planning process (Section 4.2). They define the program's tailored tasks for a specific program. The IPP lays out the overall program; the MVP comes from the Integrated Technical Planning process but is often separate plan.

#### 4.12.2.3.4 Specialty Engineering

Specialty Engineering (Section 4.8) both feeds and is fed by the Verification process. Specialty Engineering often is a source of requirements and design constraints that require Validation and Verification. In addition, Specialty Engineering analyses often are used to assist in the Verification of requirements as part of assessment. Specialty Engineering DARs are the major outputs of the Specialty Engineering process. These reports document the results of the Specialty Engineering analyses, which may result in identification and Validation and Verification of requirements. Once Verification is complete, the verified requirements are checked to ensure that the Specialty Engineering DARs reflect the Verification.

#### 4.12.2.3.5 Risk Management

Risk Management (Section 4.10) is another SE element that both feeds and is fed by the Verification process. Risk Management is able to drive the Verification of high-risk requirements. In addition, all requirements that fail to meet Verification criteria are considered a risk to the program. These requirements become inputs to the Risk Management process for mitigation.

#### 4.12.2.3.6 Interface Management

Results of the Interface Management process (Section 4.7) provide a deeper understanding of the underlying physical and functional interfaces of the system requirements. The interface documentation includes the system-level interface definitions.

##### 4.12.2.3.6.1 Lifecycle Engineering

Lifecycle Engineering (Section 4.13) is another SE element that both feeds and is fed by the Verification process. This element provides supportability, deployment and transition, real estate and disposal requirements, and design constraints. These requirements and design constraints undergo the Verification process to ensure compliance.

#### 4.12.2.4 Inputs to Verification

There are four major input categories to Verification:

- Technology
- Technical Plans
  - IPP
  - MVP
  - Program SEMP
  - NAS Architecture
- Requirements
  - Requirements documents and associated Validation Reports
  - VRTM templates populated with Requirements
- Design information and Test and Assessment articles

- Functional Architecture
- Physical Architecture
- Interface Control Documents (ICD) and IRD (if available)
- Demonstrations
- Verification Criteria
- DARs
- Updated Baselines
- Configuration Status Report
- Approved Baseline Changes

#### **4.12.2.4.1 Technology**

State-of-the-art Technology constrains the means of Verification. Therefore, it is critical that this factor be considered in the development of the Verification approach.

#### **4.12.2.4.2 Technical Plans**

These plans, developed via the Integrated Technical Planning process (Section 4.2), detail the overall vision for executing the program, including the timing and sequence of Verification. The plans that need to be collected to properly conduct Verification include the IPP, the MVP, and program SEMP. The NAS Architecture is also a valuable input in that it defines the FAA framework in which the system being verified eventually operates.

#### **4.12.2.4.3 Requirements**

Requirements documents are an output of the Requirements Management process (Section 4.3). These documents include customer operational requirements, as well as regulatory agency and statutory requirements. With Validation Reports (and associated Validation Tables) and Verification specifications included, these documents are the primary source of information for the Verification process. Phase-specific implementation teams maintain requirements documents. It is recommended that these documents include the most up-to-date information from interfaces, Functional Analyses, Specialty Engineering analyses, and system configuration.

#### **4.12.2.4.4 Design Information and Test and Assessment Articles**

This input is essential to understanding the product configuration. (Configuration Management (Section 4.11) supplies a complete description of this process.) To develop the MVP and the individual test plans, the system engineer needs any available design information, including physical architectures, drawings, interface documents, system design specifications, functional specifications, product specifications, and test equipment designs. This information also includes Specialty Engineering DARs used for the assessment. In addition, functional architectures and their associated analyses need to be available. The results of the Functional Analyses provide a deeper understanding of the underlying functions and reasons for the Requirements. ICDs, if they exist at the time of Verification, are also required. These documents provide detailed information on the interfaces involved in system operation. Part of the Validation and Verification of a system is the assurance that the Requirements for these

interfaces are correct and satisfied. The Test and Assessment Articles are the constituent pieces of the system, or the system in its entirety, on which Verification is performed.

#### **4.12.2.5 The Verification Process**

Verification is accomplished through a combination of T&E and SE Assessment. The general Verification process tasks are grouped into three distinct phases: planning, Verification activities, and documentation. Planning and documentation are common to both T&E and SE Assessment. Planning includes determination of the resources required, sequence and timing of activities, data and documentation to be produced, and establishment of the assessment criteria. The results of the planning effort are documented in the MVP. The documentation phase includes those tasks taken to ensure that evidence of completion is recorded and collated. The activity phase includes the processes or tasks in which the actual Verification methods are employed, whether they are T&E or SE Assessment. These processes are described below.

##### **4.12.2.5.1 Process for Verification by Test and Evaluation**

Specific guidelines for planning and conducting a T&E process are included in the FAA AMS Test and Evaluation Process Guidelines located under Test and Evaluation in the index of the FAST (<http://fast.faa.gov/toolsets/index.htm>).

##### **4.12.2.5.2 Process for Verification by System Engineering Assessment**

Verification by the SE Assessment is accomplished simultaneously and is fully coordinated with other SE processes—Integrated Technical Planning (Section 4.2); Requirements Management (Section 4.3); Interface Management (Section 4.7); Specialty Engineering (Section 4.8); and Risk Management (Section 4.10)—and test functions to ensure project costs, schedules, and risk implications are managed efficiently. The program plan for the Validation and Verification process is documented in specific detail in the MVP and in general in the IPP. Figure 4.12-10 depicts the overall Verification process.

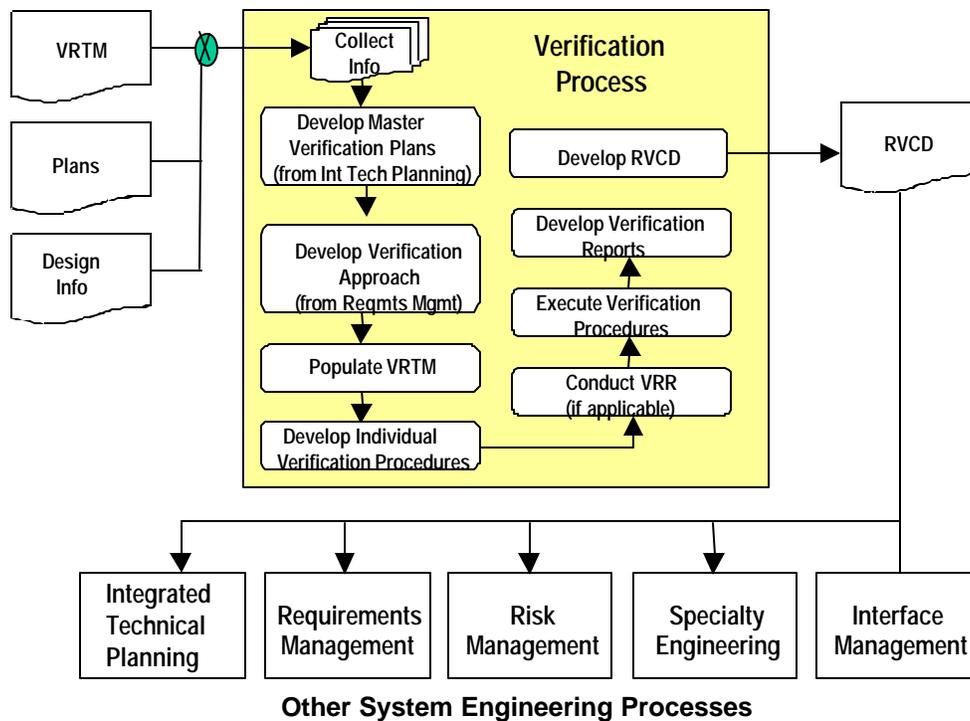


Figure 4.12-10. General Verification Process and Outputs

#### 4.12.2.5.2.1 Verification Process Purpose

Through assessment of the system product, the Verification process demonstrates that system behavior and characteristics comply with the specified Requirements. Verification provides the information required to effect the remedial actions necessary to correct nonconformance in the realized system or the processes that act on it.

#### 4.12.2.5.2.2 Verification Process Tasks

The recommended process tasks for conducting Verification of Requirements by SE Assessment appear in Figure 4.12-7 and are described in the following subsections.

##### 4.12.2.5.2.2.1 Task 1: Collect Applicable Information

At minimum, the inputs discussed in subsection 4.12.2.4 (above) shall be collected and reviewed for impacts on the Verification process. For instance, the DARs generated by Specialty Engineering (Section 4.8) may have identified special Verification procedures or needs.

##### 4.12.2.5.2.2.2 Task 2: Obtain Master Verification Plan From Integrated Technical Planning or Develop It Now

As the Verification approach is refined, the facilities, budget, schedules, personnel, test articles, instrumentation, and data necessary to accomplish the Verification events are also identified, coordinated, and approved with the appropriate decision authorities, resulting in an approved Verification plan for the program. This strategy and overall plan for the Verification process is documented in the MVP, which is delivered from the Integrated Technical Planning process

(Section 4.2) to “Task 7: Execute Verification Procedures” (subsection 4.12.2.5.2.2.7). The MVP is required to provide the content and depth of detail necessary for understanding the Verification activities. Each major activity is defined and described in detail. The MVP covers all qualification, acceptance, predevelopment, operational, and disposal Verification activities for hardware, software, and procedures. The MVP provides a general schedule and sequence of events for major Verification activities. It also describes test hardware and software, support equipment, and facilities required to support Verification activities. The MVP is developed by design, system, and test engineers with a thorough understanding of the requirements document, segment requirements and specifications, and Validation Table.

It is recommended that the following activities be completed during the planning stage:

- Identify the system and system configuration, including definition of test equipment and telemetry, facilities, and support equipment
- Identify and collate all Requirements appropriate to the (level of) Verification
- Define the specific Verification method employed for each Requirement
- Define the criteria used to evaluate the evidence from each Verification for each Requirement

#### **4.12.2.5.2.2.3 Task 3: Develop Verification Approach**

Simply put, the Verification approach is how the Requirements are going to be verified. This approach is developed in Requirements Management (Section 4.3) and documented in the VRTM. This task includes the activities of receiving, updating, analyzing, decomposing, and summarizing Requirements to ensure that they are economically and efficiently measurable and are able to be appropriately distributed for Verification planning. The purpose of Task 3 is to determine and document the Verification approach to ensure that the product is compliant with the identified Requirements.

In this step, the Verification specification (from Requirements Management) is used to develop a Verification approach for each Requirement documented in the Validation Table. The Validation Table is further refined into a VRTM. The VRTM is the heart of the Verification process. The strategy or method used to verify each Requirement is specified in a Verification Requirement, and the Verification Requirements are listed in the VRTM. The VRTM defines how each Requirement (functional, performance, design, etc.) is to be verified, the stage in which the Verification is to occur, and the applicable Verification levels. The VRTM essentially establishes the basis for the Verification program. SE and the Verification team develop the VRTM together. The T&E and the SE Assessment methods available for use are discussed in detail in subsections 4.12.2.2.1 and 4.12.2.2.2 above. Table 4.12-2 is an example VRTM. Specific guidelines for the VRTM are included in the Test and Evaluation section of the FAST (<http://fast.faa.gov/toolsets/index.htm>).

**Table 4.12-2. Sample Verification Requirements Traceability Matrix**

Section 3 Requirements Paragraph Reference for Specification SCN (Paragraph No./Title)	Requirement Description	Verification Method (Test, Demonstration, Analysis, Inspection, Engineering Analysis, Similarity, Validation of Records, Simulation, Documentation)	Verification Plan (Indicate which plan describes the Verification of the requirement)	Remarks
3.1.1.1 Aircraft I.D.		T = Test		
3.1.1.2		D = Demonstration		
3.1.1.3		A = Analysis		
3.2.1.1 System Alignment		I = Inspection		
3.3.1.1 Transmit Time		EA = Engineering Analysis		
3.3.1.2 Receive Time		SY = Similarity		
3.3.1.3 Process Time		VR = Validation of Records		
3.3.1.4 Display Time		SM = Simulation		
3.3.1.5 System Check		DC = Documentation		

**4.12.2.5.2.2.4 Task 4: Populate the Verification Requirements Traceability Matrix**

Verification is performed at all levels in a system. Each Requirement is verified either by test, SE Assessment, or both, as appropriate. As mentioned earlier, the strategy or method used to verify each Requirement is specified in a Verification Requirement, and the Verification Requirements are documented in the VRTM. It is recommended that a description of the test or SE Assessment and the criteria used to determine conformance and disposition of each Verification Requirement be included in the VRTM.

**4.12.2.5.2.2.5 Task 5: Develop Individual Verification Procedures**

This process is the detailed development of Verification procedures and resources that achieve specified Verification objectives using approved agency and regulatory procedures. Specific guidelines on content and format are in Sections 6 and 7.1 of the FAST and Test and Evaluation Guidelines (<http://fast.faa.gov/toolsets/index.htm>).

The product Verification procedures consist of step-by-step directions to conduct the actual product Verification at any level. Traceability to all Requirements in the VRTM shall be shown as an integral part of these procedures. The procedure is tailored to the Verification activity that is to be performed to satisfy Requirements and may be a test, SE Assessment, or a combination of both. The as-run and certified copy of the procedure is maintained as part of the project's archives as test or SE Assessment plans.

All Verification procedures for both hardware and software include development of test plans, procedures, and test cases. The process includes performing timing and sizing analysis

Verification at the subsystem and system levels. The results of these analyses are maintained in the test or SE Assessment plans.

The process also performs abnormal and erroneous condition testing at the subsystem and system levels. The process includes use of regression test procedures for hardware and software integration, the subsystem test, and integration and system test, including use of a core test process, if planned.

The Verification process incorporates any commercial-off-the-shelf (COTS) software or hardware in the system integration and test planning.

#### **4.12.2.5.2.2.6 Task 6: Conduct Verification Readiness Review (VRR)**

A VRR or equivalent is held before each major Verification or groups of smaller Verifications with common elements. The VRR is conducted to ensure that all SE considerations are satisfied and that the readiness of all support, test, and operational systems is in order to perform the Verification process. The VRR includes a detailed review of the status of the facilities, ground support equipment, Verification design, software, procedures, and Verification Requirements. In addition, Verification activities and schedules are outlined, and organizational/personal responsibilities are identified. Emphasis is on ensuring that all Verification Requirements identified for each Verification method or technique are included in the Verification design and procedures.

A key feature of the Verification approach is the non-advocate aspect (i.e., it is a principle of the Verification process that the person or group performing the design not execute the Verification activities). The same principle applies to planning and conducting the Verification design itself. The VRR is conducted to ensure that Verification activities are planned adequately and that risks are controlled. It is recommended that the VRR be chaired by senior personnel not associated with the program but who possess some expertise in the systems and operations under evaluation. The program implementation teams manage the VRR.

#### **4.12.2.5.2.2.7 Task 7: Execute Verification Procedures**

This task is the actual product of the Verification process (i.e., the conduct of tests or SE Assessment). The process of product Verification confirms through documented evidence of Verification activities that production-representative hardware and software are in compliance with functional, performance, and design requirements.

The Verification team performs product Verification, which consists of preparation for product Verification, execution of product Verification activities, and product post-verification and documentation. Specific guidelines for the test process are in the Test and Evaluation Guidelines in the FAST (<http://fast.faa.gov/>). When performing test Verification, the Verification team shall consult this document for specific instructions. Specialty Engineering (Section 4.8) supplies specific guidelines on conducting system (specialty) engineering assessments.

Responsibilities of the Verification team during the preparation phase of a Verification program using testing and demonstration may include:

- Design, fabrication, and/or preparation of the Verification setup
- Verification facility
- Verification fixture and/or stations

- Data acquisition, reduction, and archive system
- Verification control system
- Instrumentation system
- Design and fabrication of Verification article hardware/software
- Conduct of make-or-buy analyses for Verification setup hardware and software
- Coordination of Verification article delivery
- Coordination of Verification setup hardware/software delivery
- Coordination of support equipment and special Verification
- Preparation of Verification safety, hazard, and environmental compliance plans
- Assembly and installation of the Verification article, fixture, and setup
- Implementation of serial-numbered component installation/removal records
- Installation of Verification instrumentation
- Preparation of instrumentation installation drawings
- Implementation of instrumentation installation/removal records
- Management of Verification configuration control
- Verification articles
- Instrumentation and measurements
- Data acquisition and reduction system
- Verification support software
- Checkout and maintenance of the Verification setup hardware and software
- Coordination of Verification article configuration buyoff and/or conformity approval inspections
- Conduct of preverification conference or VRR (or equivalent)
- Management and status reporting of Verification preparation activities

During the preparation phase, quality-control members of the Verification team establish/verify conformity of Verification articles, establish/verify conformity of the Verification methods, and check/verify systems and operations.

Responsibilities of the Verification team during the product Verification execution may include:

- Maintenance of detailed Verification notes/logs, including all deviation from the MVP
- Management of Verification configuration control
- Verification facility
- Verification fixture and/or stations
- Verification article
- Instrumentation and measurements (if required)

- Data acquisition and reduction system (if required)
- Verification support software
- Coordination of Verification article configuration and/or conformity approval inspections (if required)
- Coordination of Verification witnessing
- Checkout and maintenance of the Verification setup hardware and software
- Management of calibrated equipment (if required)
- Execution of Verification in accordance with approved MVP
- Validation, collection, reduction, archive, and delivery of Verification data
- Management and status reporting of Verification activities
- Conduct of post-verification inspections
- Identification of readiness criteria for formal and informal system and subsystem test
- Conduct of unit tests on software code changes before they are incorporated; review of software code changes for correctness and the avoidance of undesired impact on other software and system variables and components

#### **4.12.2.5.2.2.8 Task 8: Develop Verification Reports**

When product Verification is complete, the Verification team conducts a post-verification review and prepares a report to disseminate the results. The Verification report is to determine compliance with the Verification Requirements.

Documentation of product Verification is completed by the Verification team and distributed to all interested parties. This documentation includes reports that detail the Verification results, including nonconformances, failure analyses, and other findings.

It is recommended that a Verification report be provided for each test and SE Assessment and, at minimum, for each major Verification activity. If testing occurs over long periods of time or is separated by other activities, Verification reports may be required for each individual Verification activity. It is recommended that Verification reports be completed within a few weeks following a test and include evidence of compliance with the Verification Requirements for which it was conducted. The Verification report documents the steps that were taken to ensure that the Verification process was followed and that the Verification decisions were sound.

Guidelines for developing and formatting specific types of T&E reports are specified in the Test and Evaluation section (specifically, Section 6) of the FAST (<http://fast.faa.gov>). For Verification by SE Assessment, it is recommended that the Verification report be documented as a DAR, as defined in Specialty Engineering (Section 4.8).

#### **4.12.2.5.2.2.9 Task 9: Develop Requirements Verification Compliance Document**

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 the 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. The RVCD contains 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 noncompliance; this section specifies appropriate reverification procedures. The RVCD is an input to the Requirements Management process (Section 4.3); decisions regarding what to do with noncompliant Requirements are made during this process.

The specific compliance information may reference a test or SE Assessment report, automated test programs, or any other data generated in the Verification process. These inputs usually occur over a lengthy period of time and may be continuous on large programs.

Up-to-date information shall be maintained in the compliance document (RVCD) for the VRR for elements already verified. The RVCD is not baselined because it is updated throughout the program's lifecycle.

The purpose of this process is to analyze the data and results from Task 7: Execute Verification Procedures" (subsection 4.12.2.5.2.2.7 above). If the Requirements have not been satisfied, coordination shall occur (with customer/stakeholder involvement, as necessary) to determine the impacts on the Requirements, design, and Verification approach. As a result of the impact analysis, compliance reports are generated, and the appropriate action(s) regarding the noncompliance are taken. This activity is iterative and shall be performed each time Task 7 is initiated. It is recommended that compliance reports include Requirements' identification information, compliance status, and Verification approach information.

The Validation and Verification process is completed when the information in the RVCD documents that all identified Requirements have been addressed by Verification activities and the product is compliant. When product Verification is completed, SE is responsible for completing/updating the RVCD.

#### **4.12.2.6 Disposal of Resources**

This process obtains formal direction or consent for shipment, contract transfer, sale, scrap, donation, or abandonment of Verification activity resources. Disposition ensures safe deactivation and disposal of all system products and processes and that Verification necessary to establish compliance with disposal requirements are finished.

Once product Verification is completed, accepted, and documented by SE and the Verification team, the Verification team is responsible for identifying unused, excess, or obsolete Verification resources. Depending on resource ownership, required disposal documentation is submitted, and resource disposal is accomplished. All resource disposal actions are documented and filed or archived, as required.

#### **4.12.3 Outputs of Validation and Verification**

The major outcomes of the Validation and Verification process are:

- Planning criteria for the Integrated Planning (Section 4.2) process to develop and complete the MVP (as well as the IPP and program's SEMP)

- Constraints that may affect Trade Studies activities (Section 4.6)
- Concerns and Issues (Appendix D) for the Risk Management process (Section 4.10) to analyze
- Outputs unique to the Validation process
  - Validated Need
  - Validation Table documented in the Validation Report
- Outputs unique to the Verification process
  - VRTM populated with Verification results
  - RVCD
  - Tools/Analysis Requirements for conducting planned Verification approach(es)
  - T&E and SE Assessment plans (internal to Validation and Verification)
  - VRRs (internal to Validation and Verification)
  - Verification documentation, including Verification reports (internal to Validation and Verification)

#### **4.12.4 Validation and Verification Tools**

There are several dedicated tools available to assist in managing the relationship between requirements, their validity, and their verification method. The selection of tool(s) shall 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](http://www.incose.org)). Smaller projects may successfully manage these relationships with a simple spreadsheet or database application instead of a dedicated tool. (The Validation Table (Table 4.12-1) and the VRTM (Table 4.12-2) further illustrate this topic.)

#### **4.12.5 Unique Tailoring Guidance**

The Verification team of a specific project may select the particular means of Verification for that project. For small projects, the project team may perform the function of the Verification team. The project team may perform both the SE and the Verification team functions. Regardless of the scope of the project and depending on the required or desired visibility into the Validation and Verification process, the project team may consider merging the Validation table, VRTM, and compliance data into one table. Such a consolidated view may be readily produced with any of the following: a simple spreadsheet application (e.g., Microsoft Excel), a robust requirements traceability application (e.g., DOORS, or Dynamic Object-Oriented Requirements System), or a relational database application (e.g., Oracle or Microsoft Access). These tools or similar tools may be used to produce this macro-level view with the capability to filter to some lesser view as needed. Table 4.12-3 illustrates this overarching consolidation view.

Table 4.12-3. Sample Validation and Verification Traceability and Compliance Table

Validation								Verification Traceability				Verification Compliance					
Source Doc (*)	PUI	Reqmt	Valid (Y/N)	Valid Source(s)	Location in Source	Corr Action	Actionee	Method				Level	Verif Reqmts Traceability	Verif Task	Plan Ref	Report Ref	Verif Status
								Test	Anal	Demo	Exam						

#### 4.12.6 References

1. Blanchard, Benjamin S. *System Engineering Management*. 2nd edition. New York, NY: John Wiley & Sons, Inc., 1998.
2. Blanchard, Benjamin S., and Fabrycky, Walter. *Systems Engineering and Analysis*. 3rd edition. Englewood Cliffs, NJ: Prentice Hall, 1998.
3. Defense Systems Management College. *Systems Engineering Fundamentals*. Fort Belvoir, VA: Defense Systems Management College Press, 1999.
4. Grady, J.O. *A Grand Systems Development Course*. Version 6.0. San Diego, CA: JOG System Engineering, Inc. (<http://www.jogse.com/home.html>)
5. *Systems Engineering Handbook*. Version 2.0A. Seattle, WA: International Council on Systems Engineering, 2004. <http://www.incose.org/>.
6. Shishko, Robert. *NASA Systems Engineering Handbook*. NASA SP-6105. Washington, DC: National Aeronautics and Space Administration, June 1995, pp.37-44.
7. *Guidelines for the Approval of the Provision and Use of Air Traffic Services Supported by Data Communications*. RTCA DO-264. Washington, DC: RTCA, Inc., 14 December 2000. (<http://www.rtca.org/>)
8. *Certification Considerations for Highly-Integrated or Complex Aircraft Systems*. ARP-4754. Warrendale, PA: SAE International, 1996. (<http://www.sae.org/>)
9. *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. ARP-4761. Warrendale, PA: SAE International, 1996. <http://www.sae.org/>.
10. *Test and Evaluation Process Guidelines*. FAA Acquisition Management System. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, July 2001. (<http://fast.faa.gov/toolsets/index.htm>)

## 4.13 Lifecycle Engineering

### 4.13.1 What is Lifecycle Engineering?

**Lifecycle Engineering (LCE) is defined as an objective process to evaluate the constraints and dependencies associated with developing and operating a product or service.** Lifecycle Engineering seeks to maximize a product's value while minimizing its cost of ownership over the entire lifecycle. 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.

Organizations are constantly looking for ways to respond to problems that become apparent with products and services and also to the need to achieve new performance levels. The approach to responding to these needs often involves system redesign and improvement of development and operational processes. In addition, the products and services often required an integrated approach to incorporating a heterogeneous collection of both legacy and emerging systems.

LCE design considerations address procurement and other issues related to the **entire product lifecycle**. It must account for the environment in which the product will operate. 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.

### 4.13.2 Why Perform Lifecycle Engineering?

LCE activities define constraints, design features, and system characteristics that are encountered throughout the lifecycle of the system. At minimum, analysis results shall be available at standard design milestones, including the preliminary and critical design reviews, and the performance reviews. LCE work supports identification of cost benefit tradeoffs, determines design progress, measures technical soundness, and supports mitigation of risk items. Stakeholders<sup>1</sup> use LCE results to ensure that the product performs as intended. LCE also supports engineering to evaluate design. The main objective of LCE is to meet the cost and performance objectives during the entire product lifecycle. Programs provide services that may be obtained from systems as well as systems having multiple system elements (e.g., system of systems). Services obtained from functions allocated to multiple systems are subject to different criteria as a result of managing multiple product baselines. Service capabilities of such "homogeneous" system configurations are constrained during development, deployment, and sustainment activities more than would be the case for those capabilities provided by service elements. LCE manages costs from inception (cradle) to disposal (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.

### 4.13.3 Lifecycle Engineering Steps

The LCE process consists of six steps—needs identification, technical assessment, technology insertion, operational assessment, performance analysis, and establishment of service

---

<sup>1</sup> It's presumed that the stakeholders are the same as identified for the Investment Analysis process; however, it is possible for stakeholders to change during the lifecycle management phase of the Acquisition Management System model.

environment (see Figure 4.13-1). Products are produced from executing these LCE steps (see Figure 4.13-2). Inputs from other System Engineering (SE) elements are required to perform LCE, and LCE products are required to effectively support other SE elements.

LCE activities support the FAA Acquisition Management System (AMS) Lifecycle phases and major decision points. LCE process steps map to these phases. LCE 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 LCE activity status. The resulting reports reflect the scope, complexity, and cost performance objectives that the planning activities provide.

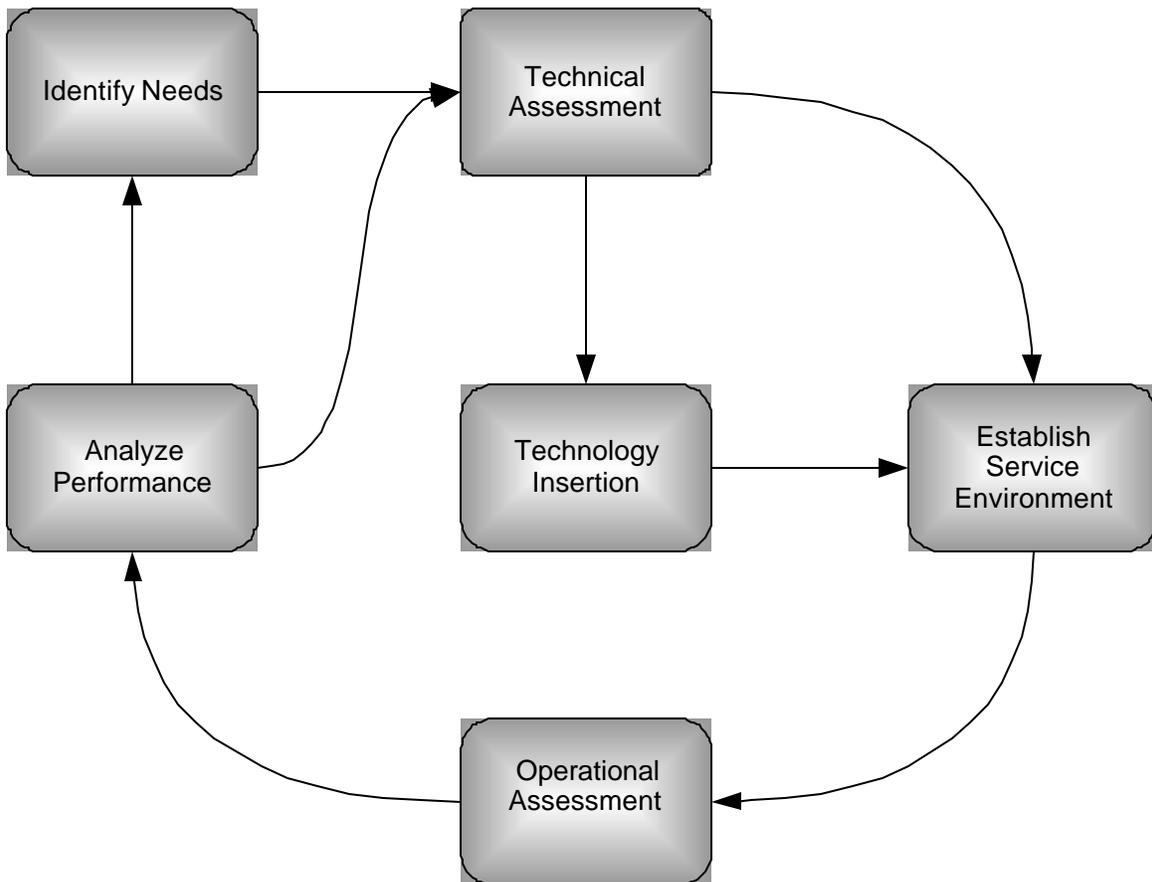
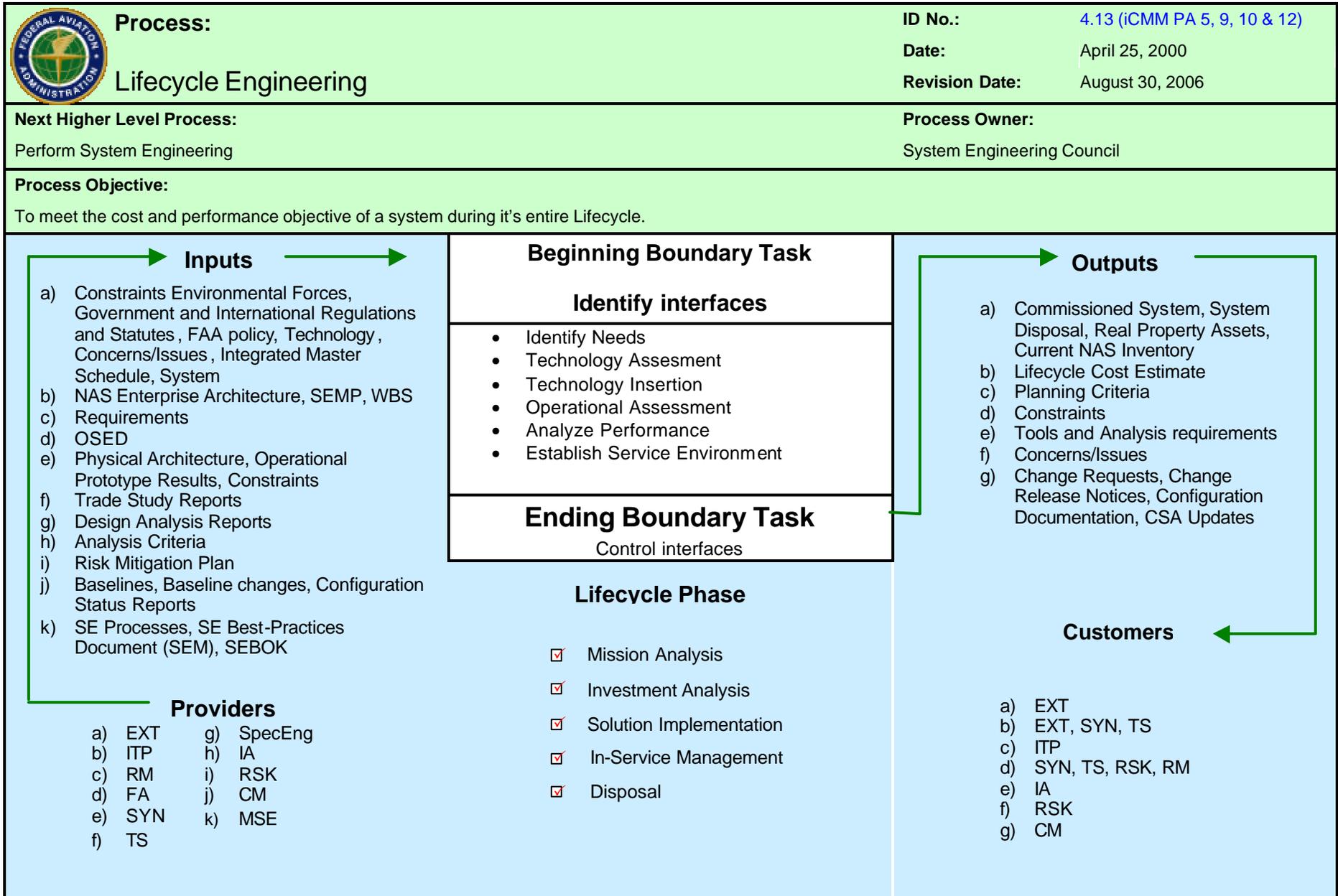


Figure 4.13-1. LCE Process Steps



4.13-3  
Figure 4.13-1. Lifecycle Engineering Process-Based Management Chart

### 4.13.3.1 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 Mission Analysis phase of the system lifecycle, and this process focuses on identifying the system capabilities needed to fulfill its mission after deployment. Identifying needs is a key part of technology insertion, update, and sustainment, and therefore it will be performed after the initial needs assessment tasks.

#### 4.13.3.1.1 Identify LCE Support Needs

LCE depends on defined service levels that detail the support needed from other systems and services in the NAS. 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 Level Mission Need during the AMS Mission Analysis phase and the program requirements. 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 that is used to deploy new components for sustaining and expanding the system and also for maintaining and repairing in-service components.

#### 4.13.3.1.2 Define Logistic Requirements

LCE defines the logistical requirements for supporting the system resources. Typically, the resources support is defined in the context of the system's overall scope and complexity during the entire system lifecycle.

#### 4.13.3.1.3 Identify Deployment Needs

Deployment of a system into the National Airspace System (NAS) will often be through phases driven by a number of factors, including budget constraints, vendor schedules, technology maturity, service environment, physical infrastructure, and logistical 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.

#### 4.13.3.1.4 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 Requirements Management (Section 4.3), Interface Management (Section 4.7), and Validation and Verification (Section 4.12)).

#### 4.13.3.1.5 Develop Earned Value Management Metrics

Identify and specify metrics for use as the Earned Value objectives for WBS items allocated to system deployment and maintenance. EVM is used to monitor costs and measure program performance. EVM offers many benefits when one measures program status against an established baseline, but it is not always the best means to compare project benefit alternatives. In evaluating project benefits, one needs to weigh such factors as the value of the various alternatives to providing NAS services and the costs associated with not providing the system at all. 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. Level-of-effort approximations should be avoided except where existing contracts require it.

#### 4.13.3.2 Step 2: Technical Assessment

Technical assessment is evaluated at the In Service Performance Review (ISPR), which is typically held every 2 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 subsection 4.2.6 in Integrated Technical Planning (Section 4.2) and Appendix C 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 use in the design under consideration, potential improvements to design performance, improvement to maintainability of the resulting system, cost-effectiveness, and maturity. 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.

##### 4.13.3.2.1 Evaluate Performance Audit

Analyze performance audit results and provide Concerns and Issues to the Risk Management element.

##### 4.13.3.2.2 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.

#### 4.13.3.3 Step 3: Technology Insertion

The need for a new technology that makes a performance or functional improvement previously not possible an 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 subsection 4.8.3, Human Factors Engineering, in Specialty Engineering (Section 4.8).)

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 commercial-off-the shelf (COTS) products, LCE should identify those items that will probably become obsolete within 5–7 years. This creates a need to develop a plan to support these items in the out years of the system's lifecycle. 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 listing of new products available in the commercial marketplace (COTS), 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, a revision of the Service Level Mission Need is required. 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 Mission 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).

#### **4.13.3.4 Step 4: Analyze Performance**

This LCE step periodically measures the system's performance against the approved baseline. The performance criteria are defined in the design. System performance is evaluated periodically.

##### **4.13.3.4.1 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.

##### **4.13.3.4.2 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 fPR (Office of Management and Budget Exhibit 300, Attachment 1) 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 maintenance support facility over all system lifecycle phases.

#### **4.13.3.5 Step 5: Operational Assessment**

At deployment, the system perfectly matches the baselined fPR. Over time, either the operational needs can change or the system deviates from the baseline due to the service environment, requiring an operational assessment. The Service 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.

Operational performance is monitored and analyzed, and data is provided as a basis for optimizing current operations and planning for future upgrades. Sustainment engineering provides COTS product obsolescence projections and determines their potential impact on system operational capability and sustainment. LCE, in its data analysis, does the following:

- Monitors and analyzes system performance
- Optimizes current operations
- Identifies technology opportunities and plan for future upgrades
- Identifies obsolescence issues and determine the impact

#### **4.13.3.6 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:

- NAILS
- Deployment and Transition
- Real Property Management
- Sustainment
- Disposal

##### **4.13.3.6.1 NAILS**

NAILS, 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 FAA. 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.

(Note: NAILS and Integrated Logistics Support (ILS) 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 terms is used during the course of procurement.)

NAILS 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 NAILS is to provide high product availability at the lowest cost.

NAILS is responsible for identification and acquisition of the support items identified as a result of an analysis of the elements. The nine elements that the 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 (Mission 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).

NAILS 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 system engineer.

#### **4.13.3.6.1.1 NAILS Inputs**

Several inputs are needed to facilitate effective NAILS 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.

#### **4.13.3.6.1.2 NAILS Process**

The typical steps involved in the NAILS process are:

- Develop NAILS constraints
- Define maintenance concept and support strategy for candidate solution
- Develop NAILS performance, cost, and schedule benefits

- Define strategy for satisfying support requirements
- Define work tasks for obtaining support
- Develop NAILS input for the procurement package
- Perform support analysis tasks
- Define maintenance support facility constraints
- Acquire NAILS assets
- Conduct In-Service Readiness Review for NAILS

#### **4.13.3.6.1.3 NAILS Outputs**

NAILS 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 the FAA will support each logistics element. This plan is developed early in the lifecycle, coordinated with system engineering, and is updated as information is further defined. It forms the basis for the contractor's Integrated Support Plan.

#### **4.13.3.6.2 Deployment and Transition**

##### **4.13.3.6.2.1 Deployment**

Deployment planning prepares for and assesses the readiness of a solution to be implemented into the NAS 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 Mission 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 the NAS.

##### **4.13.3.6.2.2 Transition**

Transition involves all work activities for installing the new system at the key site, 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 qualify them for operational service. This includes 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.

##### **4.13.3.6.2.2.1 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.

#### 4.13.3.6.2.2.2 Deployment and Transition Process

Conducting 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 followup and monitoring activities. Typical activities used to deploy and transition from the existing system to the new system are:

- Develop cutover plan for key site
- Prepare key site for new system
- Install and check out system at key site
- Integrate and test system at key site
- Prepare Independent Operational Test Readiness Declaration
- Conduct Independent Operational Test and Evaluation
- Conduct field familiarization testing for key site
- Prepare for the ISD
- Obtain the ISD
- Conduct dual operations at key site
- Commission key site into operational service
- Dispose of replaced assets at key site
- Develop cutover plan for each site
- Prepare each site for new system
- Install and check out system for each site
- Integrate and test system for each site
- Conduct field familiarization testing for each site
- Conduct dual operations for each site
- Commission in operational service for each site
- Dispose of replaced assets for each site

#### 4.13.3.6.2.2.3 Deployment and Transition Outputs

Completion of an In-Service Review Checklist and an ISD 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.

#### 4.13.3.6.3 Real Property Management

The Real Property Management process ensures recording of all real property assets that the 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 the Interim Fixed Asset System database ([http://www.faa.gov/aba/html\\_fm/ifas.html](http://www.faa.gov/aba/html_fm/ifas.html)).

##### 4.13.3.6.3.1 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.

##### 4.13.3.6.3.2 Real Property Management Process

The system 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

##### 4.13.3.6.3.3 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.

##### 4.13.3.6.4 Sustainment

Sustainment is the activity that ensures that the operational system remains at its required capability and quality.

##### 4.13.3.6.4.1 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

#### 4.13.3.6.4.2 Sustainment Process

The Service Level Mission Need (SLMN) 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 SLMN 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 as well as plan for future upgrades or replacements (Figure 4.13-3).

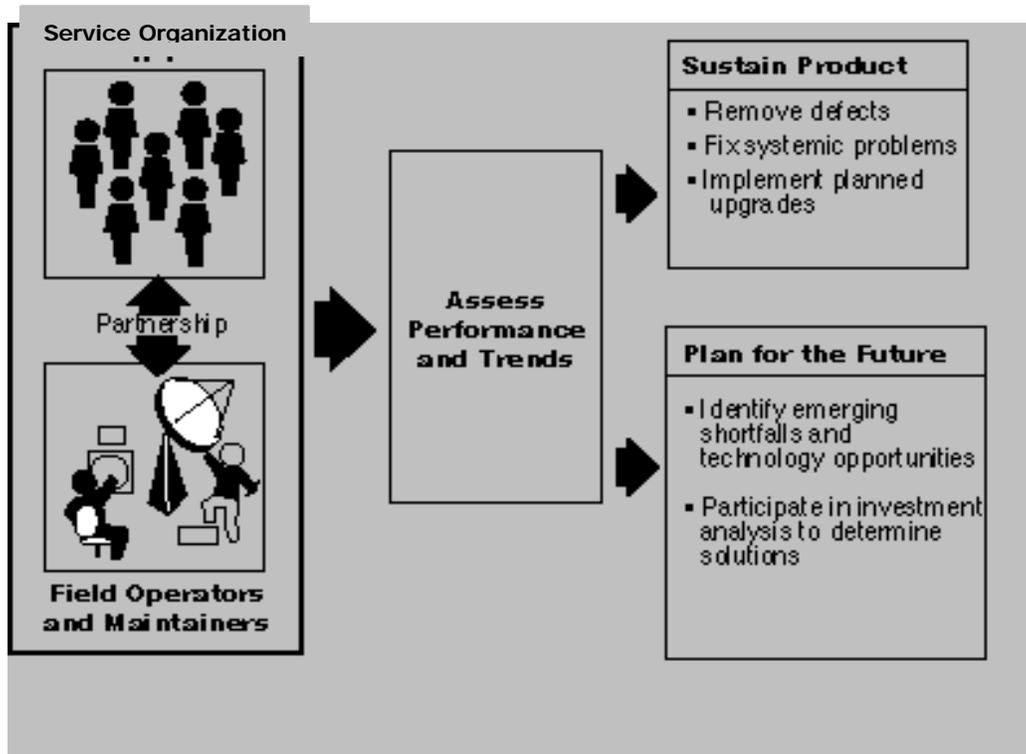


Figure 4.13-3. Assessment of Equipment Performance

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 system 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 Mission Need Statements

#### **4.13.3.6.4.3 Sustainment Outputs**

LCE produces a plan to correct systemic problems and remove defects from systems and implement planned upgrades and 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.

#### **4.13.3.6.5 Disposal**

An important element of any product's lifecycle is the process used to remove facilities from the NAS 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; or destruction of storage media and salvage of decommissioned equipment, systems, or sites.

##### **4.13.3.6.5.1 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

#### 4.13.3.6.5.2 Disposal Process

SE efforts to support disposal of a system being replaced occur during the new system's implementation phase. The Integrated Technical Planning Process (ITP) process (Section 4.2) is used to develop a Disposal Plan under 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; as well as 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 existence any hazardous materials within the system.

#### 4.13.3.6.5.3 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

#### 4.13.4 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.** This 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.** This FAA database, managed by Financial Services, records real property assets ([http://www.faa.gov/aba/html\\_fm/ifas.html](http://www.faa.gov/aba/html_fm/ifas.html)).

#### 4.13.5 References

1. *FAA Acquisition System Toolset (FAST)*. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration Federal Aviation Administration. (<http://fast.faa.gov>)
2. *Integrated Logistics Support Process Guide (ILSPG)*. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, June 2001. (<http://fast.faa.gov/toolsets/ILSPG/>)
3. Jones, James V. *Integrated Logistics Support Handbook*. Second Edition. Special Reprint Edition. New York, NY: McGraw-Hill Professional Book Group, 1998. ISBN: 0070331391.
4. *National Airspace System Maintenance Policy*. Order 6000.30C. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, 25 January 2001.
5. *Logistics Management Information*. MIL-PRF-49506. Washington, DC: U.S. Department of Defense, 11 November 1996.
6. *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.

## 4.14 System Engineering Process Management

### 4.14.1 Introduction

The Federal Aviation Administration (FAA) promotes use of the standard System Engineering (SE) processes. The processes must be continuously monitored and improved to optimize performance and ensure quality. These are institutionalized via the System Engineering Manual (SEM) and associated SE training courses. The System Engineering Council (SEC) owns and promotes use of standard SE processes and is responsible for maintaining and improving them. Figure 4.14-1 depicts the SE Process Management process.



It is recommended that the implementing organization tailor the guidance contained in this SEM to support SE process implementation. Tailoring guidance appears in subsection 4.14.6.



**Process:**

**Perform System Engineering Process Management**

**ID No.:** 4.14 (iCMM PA 21, 22, 23)

**Date:** April 25, 2000

**Revision Date:** August 30, 2006

**Next Higher Level Process:**

Perform System Engineering

**Process Owner:**

System Engineering Council

**Process Objective:**

Maintain and improve SE processes contained in SEM; Train the workforce on SE process; Incorporate process innovation.

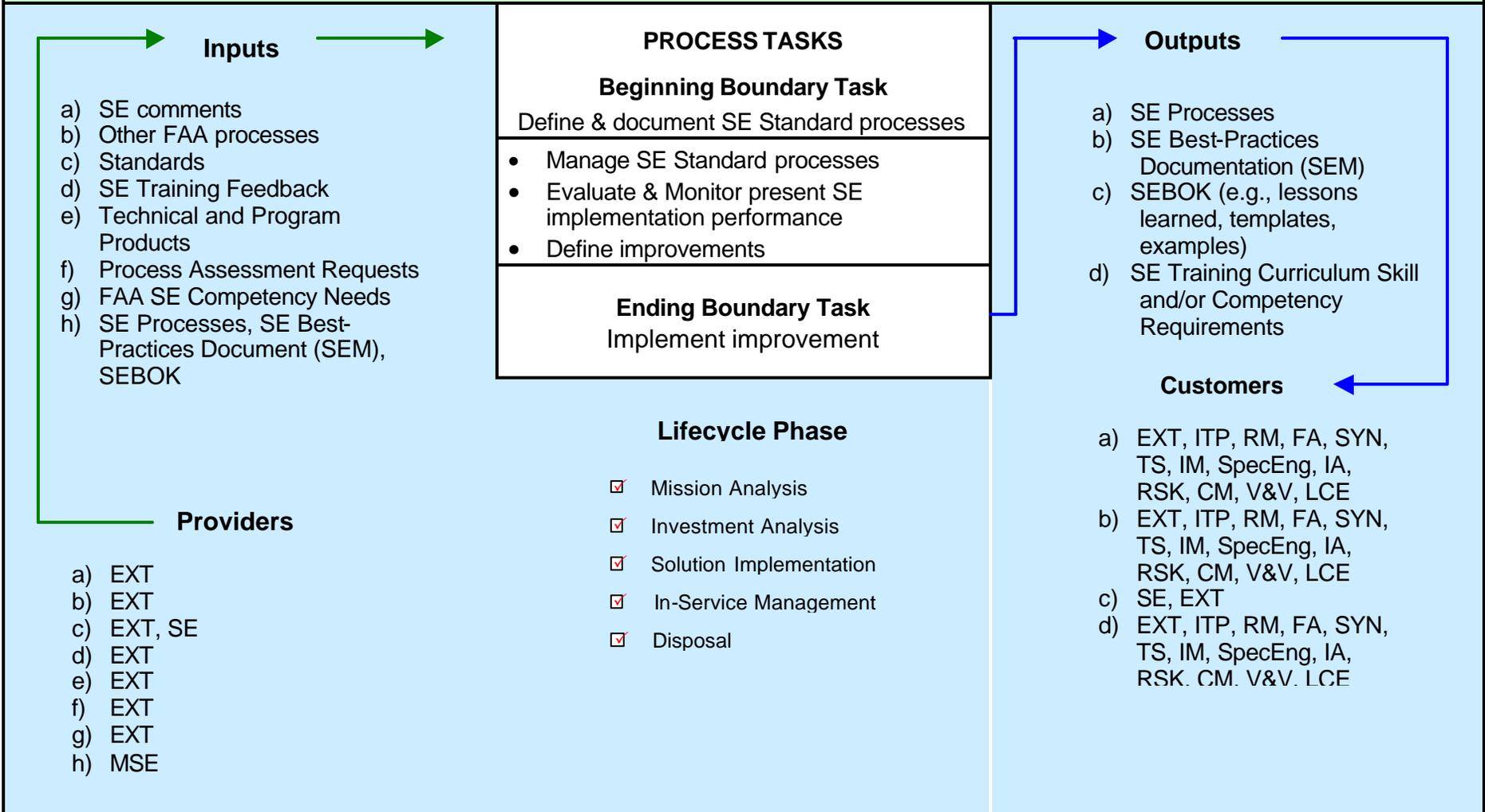


Figure 4.14-1. System Engineering Process Management Process-Based Management Chart

#### 4.14.2 Objectives of System Engineering Process Management

The objectives are:

- Maintain and improve SE processes contained in the SEM
- Manage the SE training curriculum and course content to ensure that they accurately reflect the processes in the SEM
- Sponsor training for the workforce on the FAA SE processes
- Incorporate process innovation

#### 4.14.3 Inputs

System Engineering Process Management acquires information from various sources to improve the SE processes and/or related materials.

##### 4.14.3.1 System Engineering Feedback

Feedback on SE process elements from internal FAA stakeholders, process implementers, business partners, and external SE organizations—such as the International Council on Systems Engineering—is a primary input to SE process management.

##### 4.14.3.2 Other FAA Processes

Processes within the FAA (e.g., the Acquisition Management System (AMS)) may have an impact on the SE process and may also mandate additional process metrics.

##### 4.14.3.3 Standards

Standards issued by government agencies (e.g., Office of Management and Budget and National Institute of Standards and Technology) and industry trade groups (e.g., Institute of Electrical and Electronics Engineers, Inc., and International Council on Systems Engineering) may be mandated, or they may be adopted for incorporation within the FAA SE process to enhance quality and visibility.

##### 4.14.3.4 System Engineering Training Feedback

Written and oral student critiques on the SE training courses are used as a basis for refining the SE training materials and curriculum. Attendance numbers and course demand information are collected from the instructors in accordance with SEC Standard Training Operating Procedures to determine the future direction of the training effort.

##### 4.14.3.5 Technical and Program Products

National Airspace System (NAS) SE products specified within the individual SE elements described in this document and related program implementation lessons learned are reviewed to develop and maintain SE best practices for FAA implementation. These include, but are not limited to, requirements documents such as Interface Requirements Documents, organizationally tailored SEMP, and NAS Architecture work products. In addition, these

products are used for the Technical Control and Monitoring portion of Integrated Technical Planning (Section 4.2) to assess the progress and maturity of FAA investments.

#### **4.14.3.6 Process Assessment Request Responses**

Responses to Process Assessment Requests will be periodically reviewed as submitted by FAA organizations that use SEM processes. The results are evaluated to develop a lessons learned repository to support the FAA and to adjust the processes in the SEM accordingly.

#### **4.14.3.7 FAA SE Competency Needs**

FAA-wide assessments of current and future need for SE Core Competencies are factored into enhancement of SE processes. These interdisciplinary SE resources of SE knowledge include coverage of Systems Thinking, Holistic Lifecycle View, and SE Management within the context of FAA systems. Once the shortfalls in required SE competencies, skill sets, and domain knowledge have been identified, the SEC develops a plan for eliminating shortfalls through process improvement (e.g., updates to SEM and associated training materials), internal training, mentoring, continuing education, and certification.

#### **4.14.4 Process Steps**

##### **4.14.4.1 Define and Document SE Standard Processes**

The SEM is the documented source of FAA SE processes approved by the SEC. The SEM explicitly describes the processes in a prescribed format using standard SE tools and techniques (e.g., process-based management charts and an N-squared chart).

##### **4.14.4.2 Manage SE Standard Processes**

These processes are managed as versions of the SEM and reflected in SEC-sponsored, FAA-specific SE training. Updates to the SEM, which incorporates approved updates to SE processes, are configuration controlled. The latest version is available online. FAA organizations may consider tailoring these processes during various phases of the system lifecycle. Subsection 4.14.6 describes a balanced tailoring approach. It involves an awareness of mission, environmental, and supplier constraints (e.g., standards and other FAA processes) to craft acceptable efficiencies into the nominal, rigorous process.

##### **4.14.4.3 Evaluate and Monitor Present SE Implementation Performance**

Feedback from practitioners will be solicited and evaluated to assess the effectiveness of the SE process implementation. SE products produced by services/teams implementing the FAA SEM will be reviewed to identify potential improvements for SE processes. These products will also be examined to identify implementation improvements.

Every 3 years, the SEC shall perform a detailed evaluation of the FAA SE processes and their implementation, using appropriate standard assessment models (e.g., Electronics Industries Alliance (EIA)-731 or iCMM (integrated Capability Maturity Model)). Service organizations may also request an evaluation of their tailored processes through a Process Assessment Request.

#### 4.14.4.3.1 SE Training Evaluation

SE training feedback (e.g., number of students trained, student evaluations of the courses, and assessments of applicability of course material to FAA organizations) is evaluated to assess SE training effectiveness across the FAA and to influence the future needs for the SE training curriculum. Development of the course curriculum and materials and updates are based on these evaluations.

#### 4.14.4.3.2 Required SE Capabilities

The key set of capabilities required to perform sound system engineering of the NAS is identified using the FAA SE Competency Needs. These capabilities are as follows:

- **Competency Description.** This is a refined elaboration of the SE areas of understanding described in subsection 4.14.3.7
- **Relevance.** This is a description of why this competency is significant for the target domain within the FAA.
- **Knowledge and Experience Level Criteria.** This describes the minimum conditions of maturity in that competency for various levels of expertise (e.g., awareness, supervised practitioner, practitioner, and expert).

Additionally, the availability of FAA SE resources are evaluated, focusing on levels of proficiency regarding:

- **SE Knowledge.** These are skills and techniques required to perform SE tasks (e.g., Failure Analysis, Safety Analysis, and Human Factors).
- **Basic Skills and Behaviors.** These are skills expected from a professional engineer (e.g., communication skills, teamwork, coaching).
- **Domain Knowledge.** This is knowledge of the NAS or other specific niche areas relevant to FAA mission needs.

This evaluation will be used to determine required training, continuing education, mentoring, hiring, and/or certification requirements.

#### 4.14.4.4 Define Improvement

Once a need for improvement is determined, the appropriate SE process documentation shall be analyzed (e.g., the SEM and associated training materials) to determine what specific changes must be made. The SEC is responsible for improvements to SE processes as documented in the SEM and SE training materials.

#### 4.14.4.5 Implement Improvement

The SEC shall use Standard Operating Procedures (SOP) to implement improvements and annual SE Process Improvement objectives. These SOPs ensure a consistent, formal method of process improvement.

#### **4.14.5 Outputs**

##### **4.14.5.1 SE Best Practices Documentation**

SE best practices are documented and distributed to maintain state-of-the-art SE capability in the FAA domain. Interim updates to SE processes, or improved tailoring of such processes, may be issued on an ad hoc basis. Following are examples of specific artifacts.

###### **4.14.5.1.1 SEM Updates**

New editions of the SEM are released when a revision is necessary and upon SEC approval of the incorporated SE process changes, SEM comments, and updates.

###### **4.14.5.1.2 NAS SEMP Updates**

The NAS SEMP is updated and published as necessary. This plan documents the organizations responsible for performing the SE tasks in the SEM. A program uses the NAS SEMP until the program SEMP is developed. For additional information, see Integrated Technical Planning (Section 4.2).

##### **4.14.5.2 SE Body of Knowledge (SEBOK)**

A comprehensive FAA SEBOK features the following:

- A central knowledge base for acquiring, defining, and disseminating guidance for FAA SE processes
- Reduction of redundant, divergent sources of SE knowledge
- A forum to share lessons learned about the application of SE in practice
- A starting point for learning about SE in the FAA

The SEBOK will be accessible across the FAA, and system engineers implementing the FAA SEM are encouraged to contribute to its content.

##### **4.14.5.3 SE Training Curriculum**

The SEC sponsors SE training to reflect the processes, techniques, and practices in the SEM. Updated SE course materials are distributed and taught by appropriate SE training course instructors based on the FAA SEM process descriptions or SE training feedback.

SE process training shall be consistent with the process implementation outlined in the SEM. Development of specific training shall be geared to user needs and governed by a 5-year (rolling) strategic SE training plan. The training material shall be configuration controlled, and the latest version maintained in the FAA SEBOK.

##### **4.14.5.4 Skill/Competency Requirements**

As a result of an evaluation of the FAA SE Competency Needs, a Competency Framework will be compiled describing a profile of required SE competencies, associated levels of expertise,

and a projected staffing level for these resources. These competencies will also be mapped to underlying Supporting Techniques capabilities required for each competency, and Basic Skills for enabling Supporting Techniques. This information will be used to assess the resources available and training requirements within the FAA SE community of interest.

#### 4.14.6 Guidance for Tailoring System Engineering

This SEM defines the FAA SE elements and the work products generated from these elements during each AMS phase. The 12 elements appear in Chapter 1 (Table 1.2-1). A 13th element is included to provide for process management and maintenance of the other 12 elements. These defined elements are elements of better SE practices that have been designed to be tailored. Tailoring is deletion or reduction in depth of the application of any of these 12 elements. Tailoring is also the addition of unique or special-focus elements or areas provided in organization policies and procedures or in an acquirer/supplier relationship.

Whether applied to a context that deals with systems that are large or small, hardware-intensive or software-intensive, people- or process-concentrated, many if not all of the SE elements apply. The magnitude and nature of the program determine which of the elements apply, and to what depth. It is recommended that program cost/benefit considerations be the basis for the allocation of appropriate resources, including manpower and schedule, to any process activity.

Service organizations may consider tailoring these processes during various phases of the system lifecycle. A balanced tailoring approach involves an awareness of mission, objectives, and constraints (e.g., environmental, supplier, Standards, or other FAA processes). The steps for determining the criteria for tailoring at any lifecycle phase are as follows:

1. Determine process relevance to system integrity
2. Determine process relevance to cost, schedule, and risks
3. Determine the extent of review, coordination, and decision methods
4. Determine quality of documentation needed
5. Ensure that tailoring does not increase programmatic risks

Tailoring is determined by the appropriate system engineering management authority designated in the domain (or business unit)-level or Service Organization-level SEMP. It is recommended that individual programs tailor the application of processes, tools, and techniques according to program requirements, with the appropriate SE management authority directing implementation of these processes. The chief system engineer, program manager, or other duly authorized authority makes the tailoring decision and captures the rationale for eliminating or reducing the depth of each of the SE elements in the SEMP.

It is also recommended that the assumptions, bases, and rationale for tailoring SE elements be captured in the program-level, business-level, or domain-level SEMP. The intent is not to overburden the lower-than-NAS-level organizations with mandated guidance, but to give them the prerogative to exercise judgment while remaining aware of the proven practices in the FAA SEM. This principle does not mean that large, complex programs may be de-scoped, except under the ground rules listed in this section. The following subsections give examples of specific aspects of SE processes (with referenced SEM sections in parenthesis) and how they are to be treated in a tailoring effort.

#### **4.14.6.1 Tailoring of AMS Process Phase (Chapter 3) Aspects of SE**

Chapter 3 describes the AMS phases for all programs and the SE effort to support them. It is recommended that these phases **not** be eliminated or combined on any program. However, they may be shorter. Furthermore, it is recommended that the entrance and exit criteria for any phase not be ignored. In addition, the exit reviews associated with the phases are considered mandatory. "Tailoring of Review Aspects of System Engineering" (subsection 4.14.6.3 below) discusses the SE reviews associated with the AMS exit reviews.

#### **4.14.6.2 Tailoring of Planning (Section 4.2) Aspects of SE**

It is recommended that all plans pertinent to the program be written; however, some plans may be shortened to a single page or combined in a single document. When combined, the resulting document contains the rationale and the justification for the combining. The most important plan is the SEMP, the primary product of the SE element Integrated Technical Planning (Section 4.2). The SEMP may be reduced to its essential elements, and individual entries may be as short as a single line. It is recommended that the following aspects always be retained:

- AMS phases (Section 3.2)
- SE elements (Sections 4.2 through 4.14, as tailored)
- SE specialties to be employed on the program

#### **4.14.6.3 Tailoring of Review (Subsection 4.2.6) Aspects of SE**

Two rules prevail regarding this topic: (1) It is recommended that all major reviews be performed at the end of each of the AMS defined lifecycle phases, and (2) it is recommended that reviews not be combined. However, the time between the Initial Investment Decision and the Final Investment Decision could be abbreviated if all requirements are met, depending on the nature of the program/acquisition. Additionally, a review may be shortened to an hour for a simple project. The sponsor of the review confirms the basic purpose and ground rules of the review to ensure that they meet the intended purpose. Software reviews are only required if software is selected as a solution to the system requirements (discussed below in "Tailoring of Synthesis (Section 4.5) Aspects of SE" (subsection 4.14.6.6)).

#### **4.14.6.4 Tailoring of Requirements Management (Section 4.3) Aspects of SE**

Requirements Management is an example of a fundamental process, and it is recommended that its basic principles be maintained on programs of any size. On all programs, a requirements Management tool is highly recommended, and the results are loaded into a master requirements database.

#### **4.14.6.5 Tailoring of Functional Analysis (Section 4.4) Aspects of SE**

Functional Analysis is an example of a fundamental process, and it is recommended that its basic principles be maintained on programs of any size. On all programs, it is recommended that Functional Analysis be used to derive requirements in a structured and systematic method. The depth, scope, and tools used in developing the functional architecture may be tailored according to program complexity.

#### 4.14.6.6 Tailoring of Synthesis (Section 4.5) Aspects of SE

It is recommended that Synthesis be performed to define design solutions and identify subsystems to satisfy the requirements of the verified functional architecture. Synthesis translates the functional architecture into a design architecture that provides an arrangement of system elements, their decomposition, interfaces (internal and external), and design constraints. Synthesis activities involve selecting a preferred solution or arrangement from a set of alternatives and understanding associated cost, schedule, performance, and risk implications. Depending on the type of acquisition involved (e.g., commercial-off-the shelf (COTS) items, non-developmental items, commercial hardware/developed software, and a mix of solution processes), every aspect of synthesis need not be performed, or the depth of every aspect that is performed need not be extensive.

Software is often the preferred solution to system (i.e., hardware and software) requirements. If software is required, standard software reviews and documentation are required. However, it is **not** to be assumed that, if a program is designated as a software program, then the total system aspects of SE might be ignored.

#### 4.14.6.7 Tailoring of Risk Management (Section 4.10) Aspects of SE

Risk Management is to be performed on programs of any size and throughout the lifecycle. The Risk Management process is extremely practical and adaptable to programs of any size. It is recommended that the tailoring for this process element adapt the basic process model to the program or organizational objectives. The tailoring focuses on the extent and depth that Risk Management is to be implemented, the tools to be employed, and the management-defined reporting requirements involved. A risk database is recommended for all implementations.

#### 4.14.6.8 Tailoring of Verification (Section 4.12) Aspects of SE

Verification is one of the SE basic principles—it is recommended that all requirements be verified. This is not to say that extensive testing is required, but simply that it is recommended that steps be taken to ensure that the solution satisfies the requirements. A simple analysis often provides that assurance. It is recommended that this principle not be compromised on small programs. Failure to verify requirements may cause small programs to turn unintentionally into large programs.

#### 4.14.6.9 Tailoring of Lifecycle Engineering (Section 4.13) Aspects of SE

The key to a productive and cost-effective Lifecycle Engineering process is proper tailoring so that available resources are concentrated on the data that will most benefit the program. Limitations on acquisition funding require that the lifecycle engineering effort be applied selectively in order to improve hardware design and support concepts, not merely to collect data. Specific topics of consideration should include:

- Amount of design freedom involved
- Amount of funds available
- Estimated return on investment (see Investment Analysis)
- Schedule constraints (fast-track program, compressed schedule, congressional emphasis)

- Available and relevancy of existing data

Programs are tailored in several ways. Each element of Integrated Logistics Support must be analyzed to determine what level of detail is needed to identify and procure the proper level of support. The maintenance concept (organic or contractor maintenance, remove/replace, or repair at the site level); type of acquisition (COTS or developed); documentation available from the vendor; and so forth will have an impact on the level of detail needed to support an acquisition. Programs are also tailored depending on the acquisition phase.

#### **4.14.7 References**

1. Cowper, Bennison, Allen-Shalless, R. et al. *INCOSE SE Core Competencies Framework*. International Council on Systems Engineering (INCOSE), May 31, 2005.
2. *INCOSE System Engineering Handbook*. Version 3. INCOSE-TP-2003-002-03, June 2006.
3. *Systems Engineering Capability Model*. EIA-731.1. Arlington, VA: Electronics Industries Alliance, December 1998. (<http://www.eia.org/>)