SRMGSA
Safety Risk Management Guidance for System Acquisitions

Air Traffic Organization October 2022

ALL POINTS/SAFETY
everyone. everywhere. everyday.

FAA
Air Traffic Organization

Contents

Appendices

Preface

The Safety Risk Management Guidance for System Acquisitions (SRMGSA) applies to acquisitions that have a potential effect on safety risk in the National Airspace System (NAS) when the acquired systems are operationally fielded. The SRMGSA includes information pertaining to Federal Aviation Administration Acquisition Management System changes, Next Generation Air Transportation System Portfolio Management, and Integrated Safety Management. The body of the document contains only high-level policy and guidance concerning Safety Risk Management (SRM) in acquisitions. More detailed guidance on how to conduct specific analyses/assessments is contained in the appendices of this document.

Groups within the Air Traffic Organization (ATO) (e.g., Program Offices) must comply with the SRMGSA when applying SRM to acquisitions that affect safety risk in the NAS. The SRMGSA and all other current ATO Safety Management System (SMS) policy and guidance documents are available on the ATO SMS website. Safety and Technical Training (AJI) is the focal organization for determining how system acquisitions affect safety risk in the NAS. AJI is also the Office of Primary Responsibility for the SRMGSA. All questions concerning this document should be directed to 9-AJI-SMS@faa.gov.

1 Introduction

The Safety Risk Management Guidance for System Acquisitions (SRMGSA) identifies the scope, purpose, objectives, and required activities of the Federal Aviation Administration (FAA) system safety effort as it applies to Safety Risk Management (SRM) for all system acquisitions that provide communication, navigation, and surveillance; Air Traffic Management; and other services in the National Airspace System (NAS).[1] The SRMGSA applies to all personnel performing SRM analyses/assessments on system acquisitions in the Air Traffic Organization (ATO), the Office of Airports, and other FAA Lines of Business (LOBs), as well as the Assistant Administrator of the Office of NextGen (ANG).

The SRMGSA embodies and contributes to the spirit of the FAA's safety culture. A positive safety culture places a pervasive emphasis on safety and promotes:

- An inherently questioning attitude,
- A resistance to complacency,
- A commitment to excellence,
- The involvement and accountability of management and labor, and
- The fostering of personal accountability and corporate self-regulation in safety matters.

1.1 Purpose

The SRMGSA is an FAA document that provides a framework and further process definition in order to execute SRM throughout the entire lifecycle of a system or product. The Program Safety Plan (PSP) (developed by the Program Office (PO)) and the System Safety Program Plan (SSPP) (developed by the system developer if contractually required) must use the framework of the SRMGSA to document how SRM will be conducted for the program. (Refer to Appendix A for policy on developing and implementing PSPs. Refer to Appendix B for a description of the SSPP that the system developer submits.) The SRMGSA follows systems engineering principles to achieve the SRM objectives defined in the various publications listed in Section 3.

For some acquisitions, such as those for mission support systems (e.g., Instrument Flight Procedures Automation), the PO may not be required to complete any of the safety analyses/assessments required by the SRMGSA because the system does not affect the safe provisioning of communication, navigation, and surveillance and Air Traffic Management services. The respective PO must document this determination in the program's Implementation Strategy and Planning Document in the Safety Management section.

The purpose of the SRMGSA is to meet the requirements of, and implement the policy stated in, FAA Acquisition Management System (AMS), Section 4.12, *National Airspace System Safety Management System*. This section of the AMS requires the application of a Safety Management System (SMS) and certain system development assurance practices.

FAA Order 1100.161, *Air Traffic Safety Oversight*, focuses the Air Traffic Safety Oversight Service's (AOV's) oversight efforts on the ATO's acquisition and implementation of new systems and the modernization/upgrade of legacy NAS systems. Per AOV Safety Oversight Circular 09-11, *Safety Oversight Standards*, the POs for new acquisitions are required to follow

1. For a complete definition of NAS services, refer to the NAS Requirements Document. This is the source of functional and performance requirements for FAA systems that provide air traffic control services. All operational systems' capabilities are traceable to specific requirements in the NAS Requirements Document. This document may be found at the NAS Systems Engineering Portal.

the policy of the AMS and meet the program SMS requirements. To comply, the SRMGSA emphasizes the acquisition/SRM policies and practices that must be followed. Other offices and LOBs may tailor the requirements and guidance of the SRMGSA, their SMS manuals, and other documentation accordingly.

The conduct of SRM maintains or improves the safety of the NAS by identifying the safety risk associated with making NAS changes and providing that input to decision makers responsible for managing and mitigating this safety risk. When unacceptable system[2] safety hazards are identified, the subsequent mitigations derived from the SRM process (as described in Section 3 of the ATO SMS Manual) must be translated into requirements for the acquired systems.

To assess the safety effects identified in the SRM process, the requirements set for the acquired systems must be connected to Verification and Validation (V&V) processes.[3] Without these connections, the true residual safety risk cannot be determined.

The SRMGSA defines the processes for effectively integrating system safety[4] into system changes and NAS modernization in accordance with FAA orders, the SMS Manual, and AMS policy.[5] It describes the AMS phases, organizational roles and responsibilities, program requirements, tasks, monitoring, and reporting requirements associated with performing SRM within the ATO and other organizations involved in acquisitions that affect the NAS (e.g., Aviation Safety, Office of Airports, and ANG).

The SRMGSA provides the following:

- SRM guidance for acquisitions during the following phases of the AMS lifecycle:
  - Concept and Requirements Definition,
  - Initial Investment Analysis,
  - Final Investment Analysis,
  - Solution Implementation, and
  - In-Service Management (ISM).
- SRM in support of agency Risk-Based Decision Making (RBDM).
- Specific guidance for system changes including technology refreshment portfolio projects.
- An overview of the Joint Resources Council's (JRC's) expectations regarding SRM. (Figure 2.2 shows the SRM documentation required by the JRC at each AMS decision point.)

2. The current version of FAA Order 8040.4, *Safety Risk Management Policy*, defines a system as an integrated set of constituent elements that are combined in an operational or support environment to accomplish a defined objective. These elements include people, hardware, software, firmware, information, facilities, services, and other support facets.

3. The FAA employs V&V throughout the acquisition management lifecycle in accordance with AMS V&V guidelines to support investment decisions and approvals. Verification ensures a product is built according to specifications. Validation ensures the right product is built (i.e., the product fulfills its intended use). V&V is performed early and incrementally throughout the lifecycle management process on select products, work products, and product components. See AMS, Section 2.1.6, *Verification and Validation*, for more information.

4. System safety is the process for designing safety into a product through the engineering process using a systematic approach.

5. The Assistant Administrator for ANG also uses the SRMGSA to guide his or her activities when conducting SRM.

The SRMGSA also describes the organization and responsibilities of FAA management, the ATO, and ANG in fulfilling SRM objectives. It addresses Safety and Technical Training's (AJI's) relationships within the ATO (specifically with the PO and Service Units) and with ANG for developing and approving safety documentation and accepting risk prior to JRC decisions.

1.2 Scope

The SRMGSA supports the goals of the AMS process with policy focused on service delivery and an improved transition of programs from research and development to implementation.[6] AMS policy, FAA orders, and the SMS Manual mandate a planned and organized SRM approach to RBDM that is consistent with the role of each organization in the FAA.

Leadership, direction, and guidance relating to FAA acquisition policy, research, system development, and agency information resource management require continuous collaboration among ATO organizations, Office of Airports, ANG, and other LOBs. This collaboration requires shared accountability and responsibility as these organizations engage throughout the system lifecycle. The SRMGSA encourages this collaboration, particularly within the areas of requirements management, acquisition policy, and system safety.

NAS systems not acquired through the FAA AMS process (e.g., acquired by other governments, Eurocontrol, or the Department of Defense) are outside the scope of the SRMGSA. However, they are within the scope of the FAA SMS and must follow the requirements of the SMS Manual (including submitting safety-related documentation to AOV) before they may be fielded. This includes system-constituent pieces like leased or vendor-provided services that affect the safety of the NAS.

The SRMGSA briefly discusses the analysis/assessment of proposed NAS initiatives (i.e., pre-acquisition efforts) in support of agency RBDM. An initiative can be defined as any high-level change to the operation of the NAS. The FAA Administrator may direct that any initiative be assessed for safety. This may include ANG priorities, proposed capabilities, or other types of changes being considered in the agency. Safety risk analyses/assessments for initiatives are integrated in nature and entail the review of risks induced by the impact of and interdependencies among multiple planned or fielded NAS systems. Initiatives may pose new safety risks, decrease existing risks, or impact the current risk profile of existing NAS systems and operations. Recommendations are developed as to whether the initiative should be pursued, redefined, or canceled based on the results of the integrated safety analyses.

1.3 Changes to the SRMGSA

When a change to AMS policy, the SMS Manual, or FAA management direction affects the accepted scope of performance or requirements of the SRMGSA, the SRMGSA must be revised upon agreement among the Program Management Organization; Policy and Performance, AJI-3; and the Acquisition System Advisory Group.

In addition, any safety practitioner may propose changes to the SRMGSA via the ATO SMS Mailbox or the ATO SMS Policy Management Portal. The requirements of ATO Safety Guidance (ATO-SG) ATO-SG-17-01, *Configuration Management for the Air Traffic Organization Safety Management System Policy*, apply.

6. SRM related to the ISM phase is limited to the implementation of the system. The SMS Manual provides guidance for changes to baselined systems.

2 Safety Requirements in the Acquisition Management System Lifecycle

2.1 Acquisition Management

Federal Aviation Administration (FAA) Acquisition Management System (AMS), Section 4.12, *National Airspace System Safety Management System*, contains the AMS policies for the safety management of National Airspace System (NAS) acquisitions. To meet this policy:

- Safety management must be conducted and documented throughout the lifecycle of a system,
- Safety Risk Management (SRM) must be conducted to identify safety risk(s) in the NAS,
- System development assurance must be conducted at a rigor commensurate with the severity of the potential effect(s) of hazard(s) that would result from a failure of the product. A development assurance program must implement system, electronic hardware, and software development assurance objectives and activity guidance, and
- Non-developmental product changes must be aligned with the intent of the Air Traffic Organization (ATO) Safety Management System (SMS) policy during "developmental acquisition" (i.e., qualification testing of commercial off-the-shelf items but not design reviews).

The FAA executes its acquisition management policy using the lifecycle management process, which is organized into the series of phases and decision points shown in Figure 2.1. Further details on each phase may be found at the FAA Acquisition System Toolset (FAST) website.

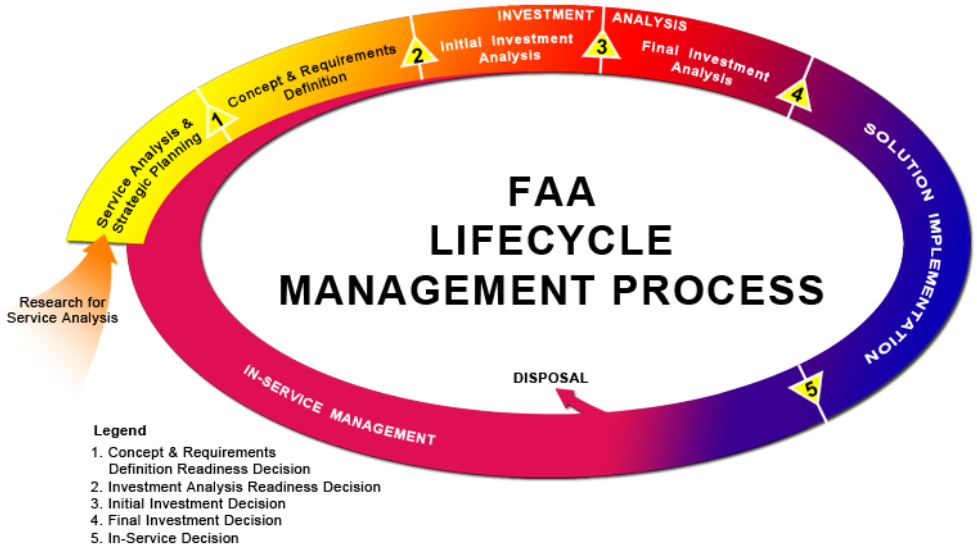

Figure 2.1: FAA Lifecycle Management Process

2.2 Integration of SRM and the AMS

The integration of SRM into the AMS process is a major objective of the ATO's SMS. This objective can be achieved by accomplishing SRM tasks using the correct system safety tools and techniques at the appropriate time to support the decisions made in the lifecycle phase. These tasks are mainly performed by the Program Office (PO) and result in products packaged in SRM documents, which are reviewed and approved prior to a Joint Resources Council (JRC) decision point or an In-Service Decision (ISD).

The circular representation in Figure 2.1 conveys the principles of seamless management and continuous improvement in service delivery over time. Application of the process is flexible and may be tailored appropriately.

The basis for analyzing and assessing a system differs for each organization. The level at which SRM is conducted also varies by organization, change proponent, and the type of change. SRM is carried out at the national level for major system acquisitions and retrofits. It may also be performed at the regional or local level to address proposed changes to equipment or Air Traffic Control procedures.

Figure 2.2 augments Figure 2.1 by showing the safety deliverables required during the FAA lifecycle management process.

See Section 2.4 for information about Technology Refreshment (TR) portfolio safety requirements.

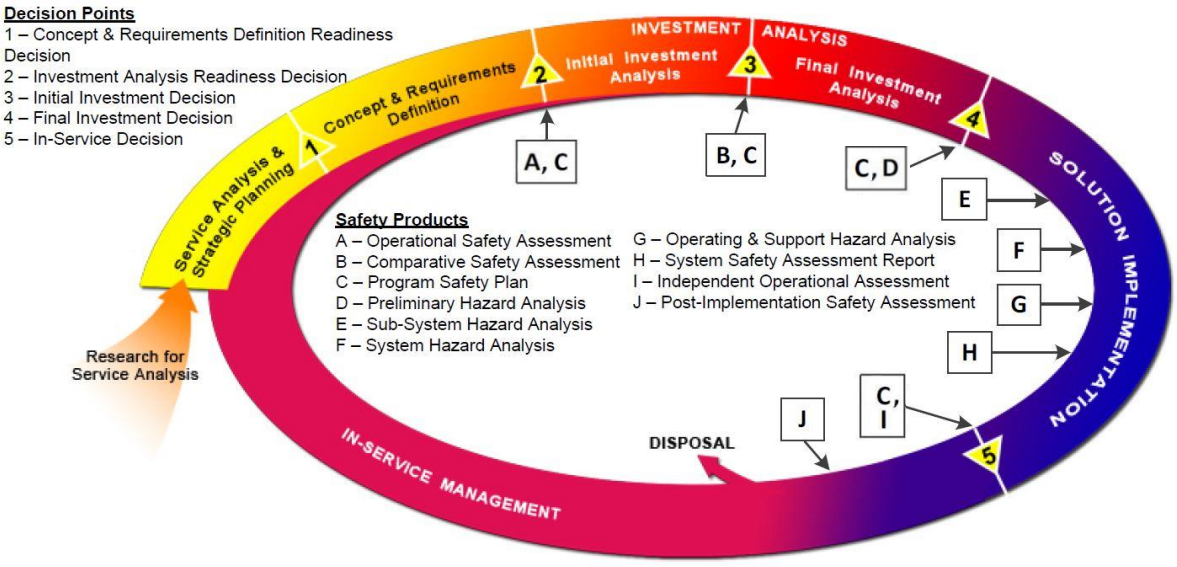

Figure 2.2: FAA Lifecycle Management Process (with Safety Deliverables)

2.2.1 System Safety Deliverables

Table 2.1 summarizes the system safety deliverables that are part of the AMS/SRM processes. Each deliverable is listed in the acquisition phase during which it must be approved.

2.2.2 Approval Authority

No individual FAA organization has total project approval authority. The PO is responsible for product approval (i.e., deciding whether the developer has complied with the contract). The JRC has funding approval (i.e., deciding whether to fund a project). The safety risk acceptor has performance approval (i.e., determining if the system's performance is acceptably safe regardless of whether the developer has complied with the contract). Safety and Technical Training (AJI) maintains the ultimate safety approval role (i.e., ensuring all system safety requirements are met). Each approver has the authority to prevent the deployment of a system. This separation of approval authority guarantees that checks and balances exist among FAA lines of business that each have different goals. Approval is a shared responsibility, and each approving entity has the right to request the necessary documentation to perform its role.

The Director of Policy and Performance, AJI-3, is responsible for approving the following safety deliverables:

- Program Safety Plan (PSP),
- Operational Safety Assessment (OSA),
- Comparative Safety Assessment (CSA),
- Preliminary Hazard Analysis (PHA), and
- System Safety Assessment Report (SSAR).

The Program Management Organization (AJM) is responsible for approving the following safety deliverables:

- Sub-System Hazard Analysis (SSHA),
- System Hazard Analysis (SHA), and
- Operating and Support Hazard Analysis (O&SHA).

Similarly, AJM is responsible for approving deliverables related to development assurance activities for system, software, and electronic hardware development.

Table 2.1 identifies the organization(s) responsible for producing the required safety deliverables. This table also includes documents that are programmatic in nature but may require safety input.

Table 2.1: ATO System Safety / Programmatic Deliverables

Acquisition Phase	Deliverables*	Reference	Responsibility	Required Approval	AMS Decision Point
Service Analysis and Strategic Planning	This phase is not covered by the SRMGSA				Concepts and Requirements Definition Readiness (CRDR) Decision
Concept and Requirements Definition (CRD)	Enterprise Architecture (EA) Safety Roadmap	AMS	Office of NextGen (ANG) / Mission Support Services (AJV) / PO	ANG	Investment Analysis Readiness Decision (IARD)
	PSP	SRMGSA Appendix A	ANG//PO	AJI	
	SRM Document: OSA	SRMGSA Appendix C	ANG/AJV/PO	AJI	
	Preliminary Program Requirements Document (pPRD)	AMS	ANG/PO	PO	
	Execution Plan (EP) (for TR portfolios)	AMS	PO	PO	
	Investment Analysis Plan (IAP)	AMS	PO	PO	
Initial Investment Analysis (IA)	Updated PSP (if needed)	SRMGSA Appendix A	PO	AJI	Initial Investment Decision (IID)
	SRM Document: CSA	SRMGSA Appendix E	PO	AJI	
	Initial Program Requirements Document (iPRD)	AMS	PO	PO	
	Initial Business Case	AMS	PO	PO	
	Initial Implementation Strategy and Planning Document (ISPD)	AMS	PO	PO/AJI**	
	Preliminary Test and Evaluation Master Plan (TEMP)	AMS	PO	PO	
	Program Management Plan (PMP)	AMS	PO	PO	
Final IA	Updated PSP (if needed)	SRMGSA Appendix A	PO	AJI	Final Investment Decision (FID)
	SRM Document: PHA	SRMGSA Appendix F	PO	AJI	
	Final Program Requirements Document (fPRD)	AMS	PO	PO	
	Final Business Case	AMS	PO	PO	
	Final ISPD	AMS	PO	PO/AJI**	
	Initial TEMP	AMS	PO	PO	
	Updated PMP	AMS	PO	PO	
	Post-Implementation Review (PIR) Strategy	AMS	PIR Team	PIR Team	
Solution Implementation (SI)	System Safety Program Plan (SSPP)	SRMGSA Appendix B	Developer	PO	Initial Operating Capability (IOC) / ISD
	Development Assurance: Accordance with Plans Reviews	SRMGSA Section 2.3.5.1.3.2	PO/AJI SCL	N/A	
	SRM Document: SSHA	SRMGSA Appendix G	PO/Developer	PO	
	SRM Document: SHA	SRMGSA Appendix H	PO/Developer	PO	
	SRM Document: O&SHA	SRMGSA Appendix I	PO/Developer	PO	
	Final TEMP	AMS	PO	PO	
	SSAR (includes Safety Requirements Verification Table (SRVT))	SRMGSA Appendix J	PO	AJI	

Acquisition Phase	Deliverables*	Reference	Responsibility	Required Approval	AMS Decision Point
	Generic Site Implementation Plan (GSIP)	FAA Order JO 6000.50	Technical Operations	PO	
	NAS Change Proposal	FAA Order 1800.66	PO	NAS Configuration Control Board (CCB)	
	PIR Plan	AMS	PIR Team	PIR Team	
	Updated PSP (if needed)	SRMGSA Appendix A	PO	AJI	
	In-Service Review (ISR) Checklist	SRMGSA Section 2.3.5	PO	AJI***	
In-Service Management (ISM)	Post-Implementation Safety Assessment	AMS	AJI	AJI	
	PIR Report	AMS	PIR Team	PIR Team	

*Safety deliverables may be tailored in a PSP.

**Sections 6.7, 7.1, 9.2, and 10.2 of the ISPD require AJI approval.

***Only Section 14 of the ISR Checklist requires AJI approval.

Note: The deliverables required by the AMS may require AJI input.

2.3 Program Safety Requirements

2.3.1 Achieving a CRDR Decision

Research and system analyses are often required during service analysis and strategic planning to mature operational concepts, reduce risk, and/or define requirements before a decision to proceed in the lifecycle management process is made. Service analysis and strategic planning policies apply when deciding whether to add a service shortfall or new operational concept to the NAS Concept of Operations (ConOps) and FAA EA.

The CRDR Decision occurs at the end of the Service Analysis and Strategic Planning phase of the AMS when an EA roadmap indicates action must be taken to address a critical mission shortfall. (Shortfalls often stem from National Transportation Safety Board recommendations or from emergent in-service operational issues due to the evolving operational environment, rather than from any latent defects of legacy NAS systems.) The CRDR Decision can also be based on some exceptional opportunities that could substantially benefit the FAA. In either case, the decision is based on speculative activities such as simulation, Functional Analysis (FA), and computer-human interface development to define potential requirements; develop operational concepts; and avoid, transfer, or reduce safety risk before entering the Initial IA phase.

The FAA SMS Committee appointed the Safety Collaboration Team to facilitate the Integrated Safety Management of pre-decisional NAS changes affecting the FAA. In doing so, the committee recognized the need to ensure that safety is not compromised when the FAA proposes pre-decisional changes that affect NAS operations.

Specific service analysis and strategic planning activities are outside the scope of the SRMGSA.

2.3.2 Achieving an IARD

The IARD occurs at the end of the CRD phase. CRD phase activities occur prior to the establishment of detailed functional requirements, baseline requirements, alternative solutions, and solution design. At the IARD, the JRC determines whether the ConOps, preliminary requirements, EA products and amendments, and preliminary program investment alternatives have been sufficiently defined to warrant entry into the Initial IA phase. The decision is made within the context of all ongoing and planned investment activities to sustain and improve service delivery. It ensures that proposals are consistent with overall corporate needs and planning.

If the concept under development requires that the proposed system, procedural change, demonstration hardware, or modified software “go live” (in a parallel, online, but nonoperational manner), SRM must first be conducted. This is especially true if the system’s “going live” involves the collection of feedback from Air Traffic personnel, suitability demonstrations, field testing, flight tests, or operational prototypes that must be exposed to field conditions only found at operational NAS facilities.

2.3.2.1 Safety Requirements

2.3.2.1.1 EA Safety Roadmap

The EA Safety Roadmap applies to the NAS as a whole and provides a broader context for Next Generation Air Transportation System changes, proactively aiming to manage safety risk in the NAS.

2.3.2.1.2 PSP

The PSP is the PO's plan for the program's SRM process. The PSP is used to ensure compliance with provisions of the ATO SMS Manual and the SRMGSA. The PO must adjust the PSP to the specific needs and SRM requirements of the program consistent with the phase of the AMS lifecycle that the program is entering. The tailoring of the PSP must be in accordance with agreements made at the Safety Strategy Meeting (SSM) (refer to Section 5.1 for details). The AJI-3 Director may require programs to identify additional features or text for inclusion.

A PSP must be developed and tailored specifically for each program requesting an IARD. The PSP supports the IARD and is completed and approved prior to the JRC Secretariat's cut-off date for the IARD. Early in the acquisition lifecycle, the PSP may be very high level as many of the program specifics are not yet known. The PO must further develop the PSP as the acquisition process matures.

The PSP must also include the PO's methodology and approach to meeting the system, electronic hardware, and software development assurance safety requirements.

At this phase of the AMS lifecycle, there could be changes to the management and safety team as the program moves from ANG to ATO control.

See Appendix A for further details on preparing a PSP.

2.3.2.1.3 OSA

The OSA is a tool for the assessment of hazard severity. The OSA identifies and assesses the hazards in a system, defines safety objectives/requirements, and builds a foundation for follow-on institutional safety analyses. The OSA provides a disciplined method of objectively assessing the safety requirements of new NAS concepts and systems, typically for Communication, Navigation, and Surveillance (CNS) and Air Traffic Management (ATM) systems. It also establishes how safety requirements are to be allocated between air and ground components and how this might influence performance, interoperability, and monitoring. Ideally, the OSA is completed during the CRD phase and must be approved prior to the JRC Secretariat's cut-off date for the IARD, which is about two weeks before the IARD JRC meeting date.

The OSA provides the system designers and management with a set of safety goals for design. It also provides an operational and environmental description, a Preliminary Hazard List (PHL) for the proposal, and an assessment of the potential severity of the hazards listed in the PHL. The results of any earlier conducted safety analyses or assessments that impact the program (such as a Functional Hazard Assessment (FHA)) (see Appendix D) are inputs to the OSA. In addition, certain planning must occur prior to the IARD, such as development of an IAP to include relevant safety information.

For replacement, removal, or reconfiguration of existing NAS systems, significant existing design, testing, field performance, NAS operations research, and/or detailed support documentation (perhaps including recent SRM documents or portfolio SRM documents) may already exist; these may apply substantially to the new proposed action. Consider an audit for applicable and reusable baseline documents and SRM documents that can form a sound basis for legacy architecture, requirements, design, performance, and known NAS constraints.

An OSA is required unless specifically waived in an approved PSP.

See Appendix C for further details on preparing an OSA.

2.3.2.1.4 System Development Assurance

Section 2.2.1.2 of the SMS Manual requires designers of NAS electronic hardware and software to design systems that will not impose hazardous conditions during abnormal performance. POs must conduct a robust system development assurance program to ensure product development is at a rigor commensurate with the severity of the resultant hazard should that product experience failure. This includes imposing system, electronic hardware, and software development assurance processes that are used to reduce systemic errors in the development processes. This may result in different Item Development Assurance Levels (IDALs) for different electronic hardware and software components.

A PO's development assurance approach is a safety requirement that must be included in the PSP approved by the Director, AJI-3. This requirement must impose which processes are being used and the associated artifacts produced from them. Also, the PSP must define the specific system functions planned and the process for imposing the Functional Development Assurance Levels (FDALs) and IDALs that are planned throughout the development.

PO planning for development assurance must begin early in the AMS lifecycle so the high-level Development Assurance Levels (DALs) can be factored into the Business Case. Typically, this occurs prior to the IARD while the OSA is being developed.

The aviation industry standards that may be used to address system development assurance are:

- SAE Aerospace Recommended Practice (ARP)[1] ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*;
- RTCA[2] DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*; and
- RTCA DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*.

DAL assignment begins with the OSA and matures as the architecture develops throughout the program. Different components may have different DALs based on their hazards.

POs for new or modified FAA CNS/ATM systems must impose a system development process such as the one outlined in SAE ARP4754A. Using this methodology, system-level FDALs would be assigned to each function based on the highest severity level within each function. Software IDALs using RTCA DO-278A and electronic hardware IDALs using RTCA DO-254 would then be allocated to each component and better aligned with system-level FDALs. The assignment of DALs is architecture dependent, and the PO should work with ANG to consider designs that not only ensure safety but also satisfy business goals.

System development assurance requirements apply to both systems being acquired via a contract with a system developer and to those being developed in-house (e.g., by the Second-Level Engineering Organization).

1. An ARP is a guideline from SAE International.

2. RTCA, Inc., is a private, not-for-profit association founded in 1935 as the Radio Technical Commission for Aeronautics; it is now referred to simply as "RTCA."

2.3.2.1.5 pPRD

The Program Requirements Document defines the operational framework and performance requirements an investment program must achieve. Preliminary program requirements specify what the new capability must do and how well it must perform its intended functions. Safety is one of the key disciplines in the AMS that must be addressed in the pPRD. Thus, safety requirements identified in the OSA become system requirements that must be included as requirements in the pPRD Safety section. The PO must plan for the fulfillment of safety performance requirements by testing and tagging requirements that are of interest to safety for special oversight. Writing a safety requirement is no different than writing other engineering requirements as described in the FAA Systems Engineering Manual.

The system-level FDALs that are initially established must also be included in the pPRD though it may be appropriate to have a stand-alone document to describe the DAL relationship among the different components and the system.

2.3.2.1.6 IAP

The IAP defines the program's scope, assumptions, investment alternatives, and organizational roles and responsibilities. In addition, there is a section of the IAP that contains the requirement for reporting the results of safety analyses/assessments as the IAP is formulated and updated while the program advances through the AMS process.

2.3.3 Achieving an IID

The IID is the point at which the JRC approves or selects the program investment alternative that best meets the required performance and that offers the greatest value to the FAA and its customers. To support that decision, the CSA is completed to inform the PO and JRC of the potential safety risks of each alternative. At this stage, the iPRD defines the program's requirements and maintains requirements' traceability against the single preferred alternative chosen at the IID. Non-preferred alternative requirements are deleted because of the IID and should not be populated in the Safety Management Tracking System. In the AMS, the Portfolio Selection Criteria Guidance for the IID shows the role played by safety and is available on the FAST website.

2.3.3.1 Safety Requirements

2.3.3.1.1 PSP

During the Initial IA phase and prior to the IID, the PO must update the PSP (if necessary) to reflect updated information (e.g., changes to the management and safety teams as the program moves from ANG to ATO control).

2.3.3.1.2 CSA

The PO must conduct the CSA, an essential assessment needed to receive an IID. The CSA defines both severity and likelihood in terms of the initial and predicted residual risk of all hazards within each solution. Likelihood is identified for the worst credible outcome of each hazard. The CSA builds upon the OSA by using the OSA's top-level FA; however, the CSA typically deconstructs the OSA by at least one level in order to expand upon the OSA's PHL. Each program investment alternative is described in sufficient detail to ensure the decision makers can understand both the proposed solutions and the hazards and risks developed.

The expanded PHL is developed from the FA or FHA, at which point each hazard's risk is assessed in the context of the alternatives. After this is done, requirements and

recommendations can be made based on the data in the CSA. The PO must write the CSA in a manner in which the decision makers can clearly distinguish the safety merit of each alternative.

A CSA provides management with a listing of all of the hazards associated with a change and a risk assessment for each investment alternative hazard combination being considered. Investment alternatives can affect cost and schedule by requiring different levels of additional safety analyses and requirements to properly address the different risk levels. Therefore, the CSA is used to evaluate the options from a safety perspective for decision-making purposes. Other considerations for decision makers (e.g., cost, schedule, training, and other implications) are not within the scope of a CSA. The PO must discuss these considerations in the IAP cost analysis and in similar Business Case reports.

A CSA is required unless specifically waived in an approved PSP.

See Appendix E for further information on preparing a CSA.

2.3.3.1.3 System Development Assurance

The system-level DALs are identified in the CSA, which may differ among investment alternatives. The DALs for the alternatives are then included in the IAP and ISPD prior to the IID.

2.3.3.1.4 iPRD

The iPRD serves for evaluating alternatives and developing the Statement of Work (SOW) and associated draft specification(s). Safety must be addressed in the iPRD; therefore, safety requirements for each alternative must be included as requirements in the Safety section of the iPRD.

2.3.3.1.5 Initial Business Case

In the Initial IA phase, the Initial Business Case may consider a number of alternative approaches for achieving the desired capability. In each case, the alternatives are evaluated against the legacy case or status quo in terms of lifecycle cost, operational benefits, safety, and risk.

2.3.3.1.6 Initial ISPD

The IID requires an initial ISPD. The ISPD provides the investment decision authority a summary of the plans for the SI phase of the proposed investment. It conveys the most critical, relevant, and meaningful information to support JRC decision making.

In the ISPD, the PO must clearly explain the scope of the safety effort and describe a high-confidence program implementation plan. Within the ATO, the ISPD is approved by both the Vice President of the organization executing the program and the ATO Chief Operating Officer. Certain sections of the ISPD are reviewed and approved by specific executives, including the Vice President of AJI.

2.3.3.1.7 Preliminary TEMP

The TEMP is the primary test management document for an acquisition program throughout its lifecycle. It delineates all activities that must be performed to achieve the goals of Verification and Validation (V&V).[3] It also documents the Test and Evaluation (T&E) methodologies that will

3. Verification is the process that ensures that the product is being built correctly (according to specifications). Validation is the process of proving that the product being built is operationally suitable and effective. Both must be successful to deploy the product.

be used to assess safety hazard controls and security risks. The preliminary TEMP describes the investment program test strategy and scope. It is developed based upon the concepts and functions documented in the iPRD prior to the IID and is not expected to contain the complete level of detail required to fully implement the T&E program.

2.3.3.1.8 PMP

The PMP defines how the service organization manages the investment program to execute the strategy recorded in the ISPD. It defines the relationships and responsibilities of key organizations that contribute to the implementation and fielding of this initiative. All investment programs that have a safety impact on the NAS are required to execute SRM as specified in the PMP.

2.3.4 Achieving an FID

The FID is the point at which the JRC approves the investment program, sometimes with Record of Decision changes and special direction. System safety has a twofold purpose leading up to the FID:

- To develop early safety requirements that form the foundation of the safety and systems engineering efforts, and
- To provide objective safety data to aid acquisition management in making decisions.

2.3.4.1 SRM Requirements

2.3.4.1.1 PSP

Prior to soliciting contractor proposals, the PSP must once again be updated (as needed) and expanded as it forms the basis of the contractor's corresponding SSPP (refer to Appendix B for more information about SSPPs). The PSP must be completed and approved prior to the JRC Secretariat's FID cut-off date.

2.3.4.1.2 PHA

To support the FID, the PO must complete a PHA to inform the JRC of the potential safety risks of the program. The required work products of the Final IA phase must be verified and validated (according to the AMS V&V guidance) prior to the FID. If the JRC accepts the recommendations, it approves the investment program for implementation; delegates responsibility to the appropriate service organization; and approves the fPRD, the Final Business Case, and the Final ISPD, all of which take safety into account.

The PHA is a common hazard identification and analysis tool used in nearly all SMS applications. Its broad scope allows for the identification of issues that may require more detailed hazard identification tools. The PHA focuses on the details of the solution architecture, including the implications for human reliability.

The PO conducts the PHA with input from the OSA, CSA, FHA, FA, and/or models such as the Bow-Tie Model. It is important to note that the OSA and CSA may not have been performed if the AJI-3 Director, in an approved PSP, waived the requirement to perform those assessments. Although an FHA and/or Bow-Tie Model are not required, they are highly recommended as tools that can assist in the hazard identification process and subsequent portions of the analysis.

The PO must conduct the PHA after the JRC has selected a single alternative as the best option. This means it is conducted after the CSA has been approved and before the FID. The SRM document must be completed and approved prior to the JRC Secretariat's FID cut-off

date. The PHA also becomes the basis of the monitoring plan that must be followed after system deployment.

A PHA is required unless specifically waived in an approved PSP.

See Appendix F for further information on preparing a PHA.

2.3.4.1.2.1 System Development Assurance

The Final system-level FDALs and software / electronic hardware–related IDALs are determined from the PHA (based on input from any conducted FA/FHA) and included in the fPRD and PSP. The impact of any changes to these DALs must be described in the Final versions of the Business Case and ISPD prior to the FID.

2.3.4.1.3 fPRD

The Safety section of the fPRD contains all new and existing safety requirements accepted by the PO. The mitigations identified in the SRM document that are allocated to the program may show up as architectural, functional, design, or performance requirements in the fPRD or as SOW tasks with deliverables. These safety items must be uniquely identified and any requirements must be included in the SRVT section of the SSAR. If all the identified safety requirements in the fPRD are eventually fulfilled and verified, then the program is expected to attain its predicted residual risk. If not, the resultant risk rating may be as high as the initial risk determined in the PHA.

2.3.4.1.4 Final Business Case

In the Final IA phase, the Final Business Case thoroughly analyzes the alternative selected at the IID including procurement alternatives.

2.3.4.1.5 Final ISPD

An FID requires a Final ISPD. The PO must update the ISPD as necessary before the FID. After the FID, the ISPD may only be modified if the program returns to the JRC to rebaseline the investment decision. Rebaselining is discouraged; therefore, the ISPD must provide high confidence, comprehensive, and contingent plans that fit within the approved baseline. Final, signed approval of the ISPD by all members of the JRC is concurrent with the investment decision.

2.3.4.1.6 Initial TEMP

The initial TEMP is required for the FID and must be approved by the PO prior to the decision point. The initial TEMP is not expected to contain the complete level of detail required to fully implement the T&E program; however, it must contain estimates of the testing scope that are sufficient to address ISPD requirements and development of T&E requirements for any proposal requests.

2.3.4.1.7 PMP

The PO must update the PMP as necessary before the FID.

2.3.4.1.8 PIR Strategy

A PIR is an evaluation tool used to assess the results of selected investment programs against baseline expectations 6 to 24 months after the program goes into operational service. The PIR's main objective is to assess an investment program, determining whether the program is achieving expected performance and benefit targets, meeting the service needs of customers,

and upholding the validity of the original Business Case. The PIR process is governed by AMS, Section 4.15.1, *Post-Implementation Review*.

The PIR Team must develop a PIR Strategy during the Final IA phase. The strategy identifies sites at which the review will be conducted, when the review is expected to occur, any limitations to the review, products of the review, and participating organizations and their responsibilities. All investment programs are potentially reviewed based on their assigned acquisition category. The AJI Safety Case Lead (SCL), PIR Quality Officer, and PO must discuss SMS considerations for inclusion in the PIR Strategy during an SSM.

2.3.5 Achieving an ISD

At the end of the SI phase, the PO must obtain an ISD that authorizes deployment of a solution into the operational environment and occurs after demonstration of the IOC[4] at the key site. The ISD establishes the foundation for the declaration of operational readiness at the key site and IOC at subsequent sites. The PO must submit an approved SRM document (typically, an SSAR, unless differently indicated in an approved PSP) at the time IOC is declared; it must be updated as necessary prior to the ISD to reflect national deployment. Additionally, prior to the ISD, all of the safety-related ISR checklist items must be closed or have an approved Action Plan.

The ISR checklist is specific to system safety and must be completed in support of the ISD. By reviewing the checklist early in a program's AMS lifecycle, the PO better understands the steps that must be completed. As programs approach the ISD, the AJI SCL, on behalf of the PO, must coordinate with the Safety Engineering Team, AJI-314, Team Manager to ensure that the system safety management portion of the checklist has been completed.

The AJI-314 Team Manager must concur with the closure of the ISR checklist items and any related Action Plans. The AJI-3 Director must approve the Action Plan as the closing authority, and he or she must concur with the closure of the Action Plan. The PO must provide the status of ISD Action Plans to the ISD Executive Secretariat for tracking until closure.

The PO must complete the suite of safety analyses delineated in an approved PSP. Typical safety analyses, some performed by the prime vendor or its subcontractor, are listed in Table 2.1.

4. The first-site IOC occurs when operational capability is declared ready for conditional or limited use by site personnel. This declaration is after the capability is successfully installed and checked out at the site and site acceptance testing and field familiarization is completed. The IOC requires satisfaction of operational requirements as well as full logistics support and training for technicians and air traffic specialists to be in place. The IOC marks the start of an operational suitability demonstration during which solution performance is evaluated under intense scrutiny to achieve full operational readiness. Additional specific criteria for achieving the IOC are defined in the acquisition program baseline.

2.3.5.1 SRM Requirements

2.3.5.1.1 PSP
Prior to the ISD, the PO must expand the PSP as needed to include any safety planning required to support the ISD and the PIR.

2.3.5.1.2 SSPP
If contractually required, the prime vendor must submit an SSPP as described in Appendix B. The PO must approve this document before development can begin.

The contractor's SSPP, when reviewed and approved by the PO, shows how the vendor or contractor intends to meet the specified safety SOW requirements (which, ideally, are based on the approved PSP).

2.3.5.1.3 System Development Assurance
Preliminary DALs are established prior to contract award based only on system functional requirements. The system development assurance activities conducted during Solution Implementation are those that are described in ARP4754, DO-278A, and DO-254 or their alternatives or whatever was required by the developer's contract.

The hazard assessments performed by the developer occur after contract award, which could be some time after the initial establishment of the system DALs. It is important to verify that the system DALs are appropriate after the hazard assessments are performed and after any change in system requirements.

2.3.5.1.3.1 Development Assurance Documents (System, Electronic Hardware, Software)
Throughout the SI phase, the PO and each developer must generate development assurance documents as required by the standards followed.

2.3.5.1.3.2 Development Assurance: Accordance With Plans
The PO must review and approve all developmental assurance documents and compare them to the standards followed to verify whether the developer complied with the appropriate level of rigor as dictated by the DALs. It is also critical that the PO work with the AJI SCL to demonstrate that the development assurance program is being (or has been) conducted in accordance with all approved plans. During an SSM, and before the Solution Implementation phase begins, the PO and the AJI SCL must discuss and agree to the nature of this working relationship. This needs to be made formal in an approved PSP.

This working relationship may take different forms depending on the complexity of the program under consideration. For instance:

- The PO may generate reports or checklists documenting their accordance with approved plans which may be submitted to the AJI SCL.
- The AJI SCL may request copies of documents to evaluate and determine whether the PO is complying with the PSP and other planning documents.
- The AJI SCL may attend periodic programmatic and engineering reviews with the PO during the Solution Implementation Phase.

2.3.5.1.3.3 Development Assurance: Audit Results

The PO must conduct audits of the contractor's development assurance activities.

Also, based on the evidence of compliance provided by the PO, the Independent Safety Assessments Team, AJI-315, may audit the development assurance process to provide an independent evaluation of (1) compliance with the PSP and development assurance plans and (2) how the PO is ensuring the traceability of safety requirements. For projects that are modifications to existing systems, the team must analyze the scope of the change and determine if the results of any previous audits are sufficient. If a new audit is deemed unnecessary, then AJI will prepare an analysis report.

2.3.5.1.4 SSHA

An SSHA is a safety risk analysis of a system's sub-systems/components typically conducted by the system developer in the SI phase at a deeper level than that of a PHA. The SSHA is typically required for cases in which system development is performed by the vendor, per the SOW. The SSHA examines each sub-system or component (including the human component); identifies hazards associated with normal and abnormal operations; and determines how operation, failure of components, or other anomalies might adversely affect the overall safety of the system. It also aids in the further determination of safety risk and the need for additional safety requirements. The output of the SSHA is used to develop safety requirements and to assist in preparing performance and design specifications. If new safety hazards are identified in the SSHA (i.e., safety hazards that were not previously described in or cannot be traced back to the PHA), then the PO must update the PHA to include them.

An SSHA is required unless specifically waived in an approved PSP.

See Appendix G for further information on preparing an SSHA.

2.3.5.1.5 SHA

The SHA is performed in the SI phase of the lifecycle of a system; it analyzes the entire system and its internal and external system interfaces. The SHA is a detailed safety risk analysis of a system's interfaces with other systems, as well as the interfaces between the sub-systems that comprise the system being studied.

The SHA is typically conducted by the system developer. The output of the SHA may be used to develop additional safety requirements and to assist in preparing performance and design specifications.

The SHA should begin as the system design matures at the preliminary design review or at the facilities concept design review milestone. It should be updated until the design is complete. If new safety hazards are identified in the SHA (i.e., safety hazards that were not previously described in or cannot be traced back to the PHA), then the PO must update the PHA to include them.

An SHA is required unless specifically waived in an approved PSP.

See Appendix H for further information on how to prepare an SHA.

2.3.5.1.6 O&SHA

The purpose of the O&SHA is to perform a detailed, systematic safety analysis addressing hazards and risk applicable to the operation and the support activities of a given system.

The O&SHA identifies hazards and risks occurring during operation of the system. This primarily encompasses the procedural aspects as well as the support functions (e.g., maintenance, servicing, overhaul, facilities, equipment, and training). Its purpose is to evaluate the effectiveness of mitigating procedural hazards (not hazards created by design). Additionally, the O&SHA must ensure that procedures do not introduce new hazards.

The timing of the O&SHA is important. In most cases, procedures are not available for review until the system begins initial use, demonstration, prototype, or initial T&E. As a result, the O&SHA is typically the last formal analysis to be completed, usually mid-way through the SI phase. The sooner the analysis can begin, the better. Even before the system is designed, an O&SHA can begin identifying hazards within the anticipated operation of the system. Ideally, the O&SHA should begin with the formulation of the system and not be completed until sometime after its initial test (which may identify additional hazards). It is critical that the design and construction of support facilities begin sufficiently before the system is ready for fielding. All special safety features must be identified early on, or the costs to modify the facilities may force POs and users to accept unnecessary risk. If new safety hazards are identified in the O&SHA (i.e., safety hazards that were not previously described in, or cannot be traced back to, the PHA), then the PO must update the PHA to include them.

The O&SHA is required unless specifically waived in an approved PSP.

See Appendix I for further information on how to prepare an O&SHA.

2.3.5.1.7 Final TEMP

The TEMP is a living document that must be updated as the program progresses with more detailed supporting information as it becomes available. The Final TEMP should be completed after design reviews, such as the critical design review, and is generally revised at major program milestones.

2.3.5.1.8 GSIP

POs must develop GSIPs[5] in accordance with the current version of FAA Order JO 6000.50, *National Airspace System (NAS) Integrated Risk Management*, for all construction and/or installation activities they sponsor. POs must develop an SRM document for any GSIP; this is typically done at the national level. Any site that deviates from the GSIP must develop an SRM document for the deviation.

2.3.5.1.9 NAS Change Proposal

Before a system can be deployed, the PO must submit a NAS Change Proposal to the NAS CCB in accordance with the current version of FAA Order 1800.66, *Configuration Management Policy*. The CCB is responsible for top-level Configuration Management (CM) of the NAS for the agency. This includes CM of the NAS Technical Architecture and traceability of requirements (including safety) from the NAS documentation/baselines to the program documentation/ baselines.

2.3.5.1.10 PIR Plan

For selected programs, the PIR Team must develop a PIR Plan prior to the ISD for the investment program under review. The plan must expand and refine the PIR Strategy by

5. A GSIP describes the steps necessary to implement a project in the NAS, regardless of where it is implemented or by whom. The GSIP is the basis for the development of location specific design and risk plans that must be developed for each project.

defining expected outcomes, planned activities, and resources necessary to complete the review. SRM input to the plan should be submitted after the SSAR is completed and approved. The AJI-3 Director must review the safety input to the PIR Plan and provide concurrence or recommendations to the PIR Team Leader and PIR Quality Officer.

2.3.5.1.11 SSAR

The purpose of an SSAR is to conduct and document a comprehensive evaluation of the safety risk being accepted before the program is deployed into the NAS. The SSAR must summarize all of the safety analyses and assessments and development assurance activities conducted by the PO during system development. The SSAR contains the SRVT. The SRVT identifies all of the safety requirements starting with the origin of the requirement (e.g., from the OSA, CSA, PHA, SSHA, SHA, or O&SHA). Prior to IOC and the ISD, the PO must conduct V&V for all safety requirements.

The SSAR must contain objective evidence of V&V closed status that may be reviewed by the AJI-3 Director upon request. AJI may also review all of the previous development assurance activities to make a Final determination that the system development assurance safety requirements have been met.

For a developer-level SSAR, each developer is required to document how they complied with safety and development assurance requirements. Each PO must provide a PO-level SSAR that documents how program-level safety and development assurance requirements were met. When the AJI-3 Director approves the SSAR, he or she is affirming that all safety requirements have been met.

The SSAR is required unless specifically waived in an approved PSP.

See Appendix J for further information on how to prepare an SSAR.

2.3.6 ISM

2.3.6.1 Post-Implementation Safety Assessment

After a system's IOC and/or ISD, AJI may perform a post-implementation safety assessment. AJI must transmit any safety-related findings to the PO for action.

2.3.6.2 PIR Report

The PIR Team must prepare a PIR Report after it completes its review. The AJI-3 Director must review the report's safety findings (including safety data that verifies whether the predicted residual risk has been met) and recommendations and provide concurrence or recommendations to the PIR Quality Officer. If the PIR reveals an increased safety risk, the risk acceptor must coordinate a reassessment to determine if changes to the safety risk mitigation strategy are necessary. An SRM panel must be convened to assess the risk of any new hazards and/or to develop additional safety requirements to ensure risk is acceptable.

After the PIR Report is completed, the PO must develop a plan outlining actions and milestones (with completion dates) to address the report's recommendations. These recommendations support the ISM phase of the AMS lifecycle and are reported to the investment decision authority; impacted Vice Presidents or equivalent; and key stakeholders, including AJI.

2.4 TR Portfolio SRM Requirements

A TR portfolio consists of two or more TR projects. Each TR project must be assigned to a sub-Acquisition Category (ACAT) of either "1" or "2" based on project cost.[6] Prior to the IARD, the TR Portfolio Manager must develop a portfolio PSP in accordance with Appendix A, which must be approved by the AJI-3 Director. To facilitate this effort, the TR Portfolio Manager must contact the AJI SCL and conduct an SSM prior to developing the portfolio PSP to assist in tailoring any safety documentation requirements. It is possible that the complexity of some TR projects may warrant the development of project-specific PSPs to supplement the portfolio PSP; this need must be detailed in the approved portfolio PSP. There may be no need to develop project-specific PSPs for sub-ACAT 2 TR projects as long as the portfolio PSP outlines the SRM and development assurance requirements for these projects. All component SRM documents must be completed prior to IARD unless a different timeline is stated in the portfolio PSP.

Each sub-ACAT 1 TR project must follow the lifecycle process presented in Figure 2.2 per the EP[7] approved by the JRC at the IARD. However, the SRM documentation required and development assurance requirements (as listed in Table 2.1) may be tailored; this will be decided during the SSM and reflected in the approved portfolio PSP (or in an approved project-specific PSP if necessary). (For example, many sub-ACAT 1 projects may not require that an OSA be conducted.) The portfolio PSP (or an approved project-specific PSP, if necessary) must specify what decision points will be held (most likely an ISD) before the product can be deployed to service delivery points. If this tailoring is not documented in the approved portfolio PSP (or in an approved project-specific PSP if necessary), then the approved portfolio PSP must be revised. Before a product can be deployed, the AJI-3 Director must approve an SSAR.

For sub-ACAT 2 TR projects, after the JRC has rendered a positive IARD, subsequent investment decisions will be made by the Portfolio Stakeholders Governing Body. This body will be different for each portfolio; it will include representatives from all applicable stakeholder organizations, and it will be chaired by the Group Manager of the organization in which the TR portfolio resides. The portfolio PSP must state what SRM and development assurance documentation will be required for each project and what safety analyses/assessments must be conducted; the safety deliverable will most likely be an SRM document with or without hazards unless otherwise specified in the portfolio PSP. Most sub-ACAT 2 projects will be approved via the NAS Change Proposals / System Safety Modification process unless otherwise specified in the EP.

The TR Portfolio Manager must report the TR portfolio sub-ACAT 1 and sub-ACAT 2 project safety status at each Acquisition Quarterly Program Review. This requirement must be stated in the TR portfolio PSP as well as in the process by which the AJI SCL will maintain safety oversight over the portfolio and the individual projects within it.

6. Since March 2019, projects above $20 million are considered sub-ACAT 1 and below $20 million are considered sub-ACAT 2. These dollar limits could change over time. Regardless, the estimated cost of a project does not determine the safety documentation required to support that project. That determination depends on the specific technical and operational nature of the project itself. Note that sub-ACAT 1 and sub-ACAT 2 projects may require different safety and acquisition deliverables.

7. The TR portfolio EP defines the portfolio's scope, schedule, cost, and performance parameters.

3 References

The current versions of the following Federal Aviation Administration (FAA) / Air Traffic Organization (ATO) orders and guidance documents supplement the Safety Risk Management Guidance for System Acquisitions:

- The ATO Safety Management System Manual;
- The FAA Acquisition Management System / FAA Acquisition System Toolset;
- The FAA Systems Engineering Manual;
- FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*;
- FAA Order 8040.4, *Safety Risk Management Policy*;
- FAA Order 1100.161, *Air Traffic Safety Oversight*;
- FAA Order 6032.1, *National Airspace System (NAS) Modification Program*;
- FAA Order JO 1030.1, *Air Traffic Organization Safety Guidance*;
- FAA Order JO 6000.50, *National Airspace System (NAS) Integrated Risk Management*;
- FAA Order 1370.121, *FAA Information Security and Privacy Program & Policy*;
- FAA Order 9550.8, Human Factors Policy;
- Air Traffic Safety Oversight Service (AOV) Safety Oversight Circular (SOC) 09-11, *Safety Oversight Standards*;
- AOV SOC 07-02, *AOV Concurrence/Approval at Various Phases of Safety Risk Management Documentation and Mitigations for Initial High-Risk Hazards*;
- AOV SOC 07-05, *Guidance on Safety Risk Modeling and Simulation of Hazards and Mitigations*;
- ATO Safety Guidance (ATO-SG) ATO-SG-17-01, *Configuration Management for the Air Traffic Organization Safety Management System Policy*;
- Human Factors Job Aid;
- NAS Enterprise Safety Handbook;
- RTCA[1] DO-248C, *Supporting Information for DO-178C and DO-278A*;
- RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*;
- RTCA DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*;
- RTCA DO-330, *Software Tool Qualification Considerations*;
- RTCA DO-331, *Model Based Development and Verification Supplement to DO-178C and DO-278A*;
- RTCA DO-332, *Object Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*;

1. RTCA, Inc. is a private, not-for-profit association founded in 1935 as the Radio Technical Commission for Aeronautics; it is now referred to simply as “RTCA.”

- RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*;
- SAE Aerospace Recommended Practice (ARP)[2] ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*; and
- SAE ARP4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*.

2. An ARP is a guideline from SAE International.

4 Roles and Responsibilities

The organizational roles and objectives involved in the Federal Aviation Administration (FAA) Acquisition Management System (AMS) are designed to ensure the accomplishment of the following objectives:

- Systems under consideration for inclusion in the National Airspace System (NAS) are evaluated systematically (i.e., from vertical, horizontal, and temporal perspectives) and at an appropriate time to assist in decision-making.
- Initiatives are assessed by conducting Integrated Safety Management in support of agency Risk-Based Decision Making; results are incorporated into the Safety Risk Management (SRM) activities for individual systems, as appropriate. Integrated Safety Management is conducted to provide a complete picture of the potential safety risks of fielding a particular NAS capability (see Sections 4.2 and 4.4).
- Appropriate safety requirements consistent with the AMS are developed for each solution and best systems/safety engineering practices are used in the earliest possible phases of system development.
- Safety performance targets and monitoring plans are established, and monitoring activities are conducted in accordance with the Air Traffic Organization (ATO) Safety Management System (SMS) Manual.
- Hazards are analyzed and assessed for safety risk. Risk associated with known safety issues is actively controlled and mitigated to an acceptable level, as necessary.
- Consideration of safety risk, an integral part of each AMS decision, is required for every Joint Resources Council (JRC) decision in which resources are committed to the development and acquisition of systems.
- FAA resources are properly focused on controlling and mitigating the highest risk elements and hazards of the NAS and the systems under development.

To accomplish these objectives, any organization proposing a change to the NAS must commit the necessary resources to ensure that all required safety assessments/analyses and documents are completed.

The roles and responsibilities of each organization involved in implementing SRM in system acquisitions are detailed below. A complete description of roles and responsibilities for the JRC and organizational entities can be found on the FAA Acquisition System Toolset (FAST).

4.1 JRC Executive Secretariat

The JRC Executive Secretariat maintains the AMS-based JRC Readiness Criteria Checklist, which ensures that the appropriate SRM documents required for all investment decisions have been coordinated with Safety and Technical Training (AJI). Policy and Performance, AJI-3, must verify the completion of SRM documentation for programs progressing through the AMS and advise the JRC Secretariat as to the decision to be made.[1] The JRC has funding approval for the FAA and can decide whether or not to fund a project.

1. The SRM documentation is not forwarded to the JRC Executive Secretariat for review. The JRC Executive Secretariat only requires a notification from AJI-3 that the program has met its SRM obligations, as required by the AMS.

4.1.1 Portfolio Stakeholders Governing Body

For sub–Acquisition Category 2 projects within a Technology Refreshment (TR) portfolio, after the JRC has rendered a positive Investment Analysis Readiness Decision, subsequent investment decisions will be made by the Portfolio Stakeholders Governing Body. This body will be different for each portfolio; it will include representatives from all applicable stakeholder organizations, and it will be chaired by the Group Manager of the organization in which the TR portfolio resides.

4.2 Assistant Administrator for the Office of NextGen and Next Generation Air Transportation System Portfolio Management

The Office of NextGen (ANG) is charged with conducting research, developing prototype systems, planning acquisitions and supporting activities, performing Test and Evaluation (T&E), and guiding enterprise systems engineering, all for the purpose of modernizing the NAS. ANG provides a suite of SMS tools and resources that address the challenges of modernizing the NAS toward a more integrated system-of-systems, while maintaining or enhancing its safety. The suite of tools includes the following:

- An Integrated System Safety Assessment (ISSA) assesses changes in safety risk resulting from the implementation of the Next Generation Air Transportation System (NextGen) Operational Improvements (OIs). The ISSA Report serves as a foundational safety document that feeds into other safety analysis/assessment activities through the course of the program lifecycle process.
- A Service-Level Safety Assessment is a means to assess current safety risk and provide a baseline for subsequent changes to the NAS.
- The Hazard Enterprise Assessment Tool (HEAT) guides SRM panel participants step-by-step through the SRM process. The tool facilitates a more robust, accurate, and comprehensive safety analysis by providing a standard hazard taxonomy and automating complex risk calculations based on National Transportation Safety Board safety data and Subject Matter Expert (SME) input.

4.2.1 ANG Enterprise Safety Team

The Enterprise Safety Team (EST) consists of safety SMEs from the Enterprise Safety Branch, ANG-B32, who oversee ANG SMS compliance, develop tools and processes, and provide guidance for supporting the ANG SMS. The EST is responsible for the safety analysis of NextGen projects, ensuring safe and successful implementation in future NAS environments. Furthermore, the EST conducts safety analyses on planned NAS changes associated with OIs to identify potential safety hazards and safety benefits.

The EST collaborates with its partners and stakeholders to devise strategies for mitigating safety risk and improving safety benefits for future NextGen capabilities. Moreover, the EST develops methodologies and provides guidance on Integrated Safety Management and incorporating SMS standards and practices throughout ANG functions.

The EST's roles related to NAS acquisitions include:

- Conducting enterprise-level safety assessments for air traffic management services and future NextGen capabilities;
- Developing and providing guidance on safety assessment methodologies in support of Risk-Based Decision Making and Integrated Safety Management;

- Serving as the safety Point of Contact (POC) for all SMS matters related to ANG;
- Overseeing the SRM process for ANG activities, including Research and Development and Trials, Tests, Demonstrations, and Prototypes (TTDP);
- Reviewing and concurring with AMS Program Requirements Documents (PRDs) to ensure safety requirements are consistent with SRM documentation; and
- Maintaining the NAS Enterprise Architecture (EA) Safety Roadmap.

4.2.2 Portfolio Managers

The NAS Segment Implementation Plan (NSIP)[2] describes OIs and the increments necessary for developing, integrating, and implementing NextGen capabilities. The NSIP is organized into individually managed portfolios that encapsulate capabilities with a common benefits pool, consisting of multiple organizations with implementation responsibilities. ANG Portfolio Managers facilitate the implementation of new capabilities by coordinating key activities, including relevant SRM efforts.

Specifically, Portfolio Managers must:

- Include the appropriate SRM efforts required by the Safety Risk Management Guidance for System Acquisitions (SRMGSA) and/or the *NAS Enterprise Safety Handbook* as stated in Project-Level Agreements;
- Support the EST by providing program/project schedules, technical documentation, and SME support for conducting ISSAs on OIs;
- Collaborate with the EST and Program Offices (POs) on developing and implementing safety recommendations from ISSAs to mitigate potential safety risks and/or improve safety benefits associated with OIs;
- Inform POs about leveraging ISSA Reports as the baseline for initial program-level SRM, in accordance with Joint Resource Council (JRC) checklist requirements (see Section 4.1); and
- Ensure all ANG-funded activities (e.g., TTDP) are conducted in compliance with SRM requirements.

4.2.3 T&E Teams

ANG T&E activities verify and validate program safety hazard–related requirements. The conduct of T&E activities may also identify new safety hazards that have been overlooked by the program. The T&E teams develop the Test and Evaluation Master Plan to ensure that appropriate testing methodologies are planned for and followed. The T&E teams support and oversee the planning, conduct, and reporting of Development Testing (DT) and Operational Testing (OT). The DT and OT phases support the identification and evaluation of potential safety hazards and safety hazard–related requirements.

The T&E results must be included in the Verification Requirements Traceability Matrix (VRTM) to provide the pass/fail status of safety hazard–related requirements. If T&E activities identify a new hazard, it must be clearly noted in a Test Report, and the AJI Safety Case Lead (SCL) must be notified for guidance on the prescribed SRM action. The T&E teams report findings to

2. The NSIP is the FAA's blueprint for achieving NextGen OIs. Along with outlining improvements, the NSIP addresses current investments and activities that help sustain the NAS.

the PO. The Program Management Organization (AJM) includes test results in the System Safety Assessment Report (SSAR) and then works with AJI for further action. The PO uses the data from the test reports and VRTM to update the Safety Requirements Verification Table for the SSAR.

4.2.4 Human Factors Specialists

ANG Human Factors (HF) specialists address human capabilities and limitations within the development of systems and equipment, procedures, tasks, training, personnel selection, and more. HF specialists[3] are distributed across the FAA but are primarily in ANG, Aviation Safety (AVS), and the ATO. Their roles typically concentrate on research or application (or both), with a focus on NAS safety and efficiency through human performance.

Current capabilities are typically developed independently of others, such that analyzing the integration of capabilities from the human operator or maintainer perspective is critical, yet not fully understood prior to operation. Enterprise-level safety analyses should address how new capabilities affect humans in the context of their overall tasks; this topic can best be determined by ensuring that qualified HF specialists participate. Operational SMEs can also provide valuable insight, but they should not be considered substitutes for consulting qualified HF specialists.

HF specialists support various Enterprise Safety activities, such as:

- Serving as POCs to other FAA HF specialists with specific experience;
- Identifying other HF resources, such as regulations, policies, and standards;
- Conducting HF research to support safety analyses and mitigations; and
- Participating in safety analyses directly, including T&E.

4.3 AVS

AVS includes the Air Traffic Safety Oversight Service (AOV), which provides independent safety oversight of air traffic services. AOV oversees the SRM process for system-oriented safety standards related to the acquisition and implementation of new systems (including modernization/upgrades of legacy NAS systems) in accordance with the current versions of FAA Order 1100.161, *Air Traffic Safety Oversight*, and AOV Safety Oversight Circular (SOC) 09-11, *Safety Oversight Standards*.[4] It is important to note that AOV must approve any mitigations identified in an SRM document that lower the safety risk of hazards initially identified as high risk before those mitigations may be implemented and the system(s) fielded.

4.4 Safety Collaboration Team[5]

The FAA Safety Collaboration Team (SCT) was appointed by the FAA SMS Committee[6] to serve as the technical advisory body to the committee and to facilitate the safety risk

3. The expectation is that the government HF focal points will reference FAA Order 9550.8, *Human Factors Policy*, the Human Factors Job Aid, and FAA HF standards (FAA HF-STD-001 and FAA HF-STD004) as well as be fully informed about the requirements and guidance in AMS, Section 4.7, *Human Factors*, and the FAST HF website.

4. AOV SOC 09-11 provides systems-oriented information and guidance material that may be used by the ATO to develop and implement procedures to comply with FAA Order 1100.161.

5. The contents of this section are taken from the Safety Collaboration Team Charter signed June 5, 2018.

6. The FAA SMS Committee is a cross-organizational coordinating body that focuses on safety and safety management. The purpose of the FAA SMS Committee is to assist SMS implementation, planning, and improvement by recommending policy and process guidance across the FAA. All such guidance must be approved by the FAA SMS Executive Council. The FAA SMS Committee also coordinates cross-organizational safety issues and safety management concerns in the FAA.

assessment of planned NAS change concepts as a means to prevent the potential onset of safety hazards and/or unacceptable risk in NAS operations.

The SCT is a team of safety professionals from various FAA Lines of Business (LOBs) and Staff Offices whose primary objectives are to:

- Provide cross-organizational SRM consultation services for planned NAS change concepts;
- Facilitate safety risk assessments for planned NAS changes or other agency safety issues that span across LOBs in accordance with the current version of FAA Order 8040.4, *Safety Risk Management Policy*; and
- Foster collaboration that supports the advancement and common understanding of cross-organizational safety management among safety professionals.

The SCT also assists with the identification and analysis of enterprise-level safety issues within the NAS environment. This could include facilitating cross-organizational safety assessments that can be used as input data for the safety risk analysis of new system acquisitions or operational changes and provide FAA decision makers with information to make risk-informed decisions.

If necessary, the SCT establishes standing workgroups to address safety issues outside the scope of FAA Order 8040.4 requirements. The workgroups may perform the following tasks:

- Conduct research and analyses to identify safety issues and/or trends.
- Develop a detailed recommendations report based on the research and data analysis results.
- Conduct peer reviews on pertinent safety documents including the recommendations report.
- Present the recommendations report to the SCT Chairs for their consideration and subsequent submission to the FAA SMS Committee, risk-based decision makers, applicable acquisition programs, or operational change proponents.

The processes and procedures used by these workgroups and the SCT are beyond the scope of the SRMGSA. However, the outputs of these workgroups and the SCT may be useful to the PO when conducting SRM.

4.5 ATO

Figure 4.1 summarizes the ATO's safety roles and responsibilities, which are detailed in the sections below.

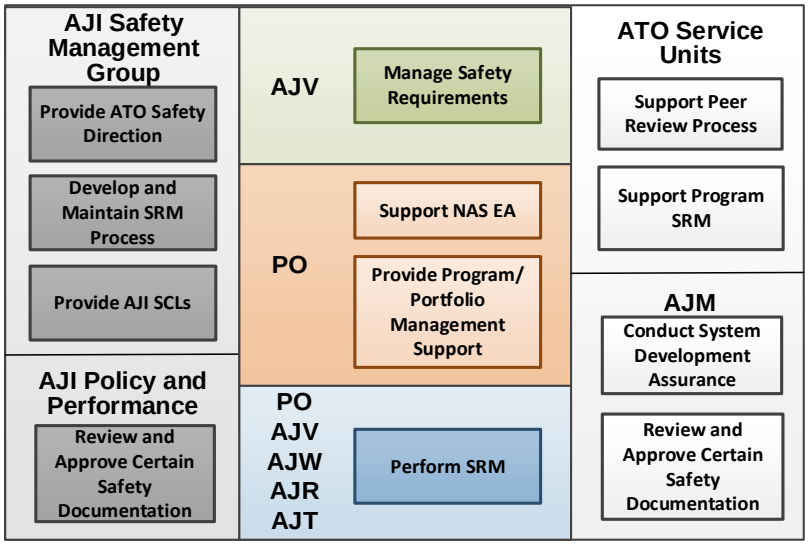

Figure 4.1: ATO Roles and Responsibilities

4.5.1 Service Unit Roles and Responsibilities

Depending on the acquisition phase of the program, the PO (whether in AJM, Mission Support Services (AJV), or Technical Operations (AJW)) has the responsibility to ensure that SRM has been conducted on NAS changes and the necessary documentation has been prepared. The PO is supported, as appropriate, by SMEs from the Service Units (SUs). AJI-3 personnel also support the PO in preparing the safety documents and representing their functional discipline at reviews. SU representatives to the PO ensure that the SU Vice Presidents are informed of the risks involved with a proposed change to the NAS and recommend that they approve SRM documentation and accept risk in accordance with the SMS Manual, as necessary.

Managers within the SUs may be designated as safety risk acceptors. The safety risk acceptor has safety performance approval authority for any NAS change or system deployment and may decide that the system's safety performance is acceptable regardless of whether the developer has complied with the requirements of the contract.

4.5.2 AJV Roles and Responsibilities

AJV breaks down the FAA's Concept of Operations into operational needs. These operational needs are then aligned with new/existing OIs or current operations and prioritized and allocated to portfolios. The operational needs are broken down into initial operational requirements, including safety requirements, which may or may not result in a need for an acquisition. AJV must validate complete sets of functional, design, and performance requirements for the PO.

4.5.3 PO Roles and Responsibilities[7]

The PO must conduct SRM on NAS changes. The PO must monitor safety requirements of acquisition programs to ensure the requirements are met through design audits, developmental and operational tests and evaluations, and performance checks (most notably before the Initial Operating Capability and the Post-Implementation Review, if applicable). The PO must also identify programmatic risks (e.g., cost or schedule) that could affect safety.

Within the ATO, the PO coordinates the NAS EA[8] support effort for all roadmaps (except the safety roadmap) by providing the alignment of systems and technologies with the mission/business leads. This includes planning for SRM application in all ATO-managed acquisition programs.

Many of the functions performed by successful acquisition POs are beyond the scope of the SMS and the SRMGSA. However, some of these functions are relevant to fulfilling the SRM requirements as they relate to acquiring new solutions. Among them are planning and resource management, which include ensuring that SRM considerations are part of the decision-making process. The PO must ensure that SRM policy and guidelines are followed.

The PO may be supported by a Program Safety Team (PST). When forming a PST, the PO should choose people who are able to:

- Communicate with program stakeholders,
- Understand program objectives,
- Understand program plans and acquisition strategies,
- Develop strategies and action plans for the safety compliance of the program,
- Define safety input into program plans and supplier agreements,
- Perform safety analyses,
- Track and analyze safety compliance for the program,
- Implement mitigation steps as required, and
- Report program safety activities and monitoring results.

The PO must ensure that all members of the PST receive SMS training and understand the SRM process.

The PO is responsible for verifying that system developers comply with system development assurance standards, the system specifications, and any other standards. This is done by:

- Producing a Program Safety Plan (PSP) that describes all the reviews, checklists, and activities the applicant will perform to ensure the developer complies with system development assurance standards (Appendix A);
- Ensuring the contract contains the development assurance requirements with which the developer must comply;

7. For information regarding the roles and responsibilities of POs not part of the ATO, contact the Safety Engineering Team, AJI-314.
8. The NAS EA contains roadmaps that describe the transition from the “as-is” to the “to-be” environment (i.e., from the current environment to the planned one). Roadmaps align the FAA’s mission, benefits, and capabilities with its investments. The EA also contains architectural “as-is” and “to-be” views that govern the expected architecture, threaded features, levels, functional flow, dependencies, and holistic performance of the NAS to be allocated among integral groups of dependent NAS systems. EA views, more so than roadmaps, help control the impacts of changes among NAS systems.

- Performing reviews and audits of the developer's Quality Assurance (QA) activities;
- Spot-checking the engineering products to verify the QA work;
- Approving all engineering documentation generated by the developer; and
- Establishing a working relationship with the AJI SCL during the Solution Implementation (SI) phase of the program.

For SRM efforts conducted as part of the AMS process, the PO should hold a meeting with the ANG EST[9] (see Section 4.2.1) to review relevant enterprise safety assessments and HEAT reports and to assist with SRM compliance. Also, when appropriate, the PO should coordinate SRM efforts with Second-Level Engineering.

The PO must include the program's SRM efforts in the total scope of work to be carried out by the project team to accomplish the project objectives and create the required deliverables. This must be reflected in the project's Work Breakdown Structure.[10]

4.5.3.1 PST

A PST is a resource provided by the PO to support the safety efforts of an acquisition throughout the AMS lifecycle. The composition of the PST depends on the size and complexity of the program under consideration.

The PST, in conjunction with the AJI SCL, defines the planned safety effort and ensures that the required safety products are prepared to support the JRC decision process.

The PST must:

- Provide a central point of contact to coordinate all safety analyses throughout the program's lifecycle;
- Participate in Safety Strategy Meetings (SSMs) to determine the safety effort required in support of the AMS milestone decisions;
- Support the safety analyses in accordance with the guidelines in the AMS, the SMS Manual, ATO Safety Guidance (ATO-SG) documents, and the SRMGSA;
- Submit the proposed PSP and completed SRM documents to the AJI SCL for review and coordination to ensure timely decisions in support of JRC milestone decisions;
- Ensure the developer's contract includes provisions to support AMS development assurance safety requirements;
- Review all development assurance documents to include required lifecycle data, as applicable, and provide evidence of process compliance to AJI-3;
- Enter required safety documentation into the Safety Management Tracking System (see Section 8.5 for more information);

9. The ANG EST develops processes and provides guidance that enforce SMS compliance for all of ANG. The ANG EST is responsible for assessing the safety of highly complex and interrelated systems in the NAS and identifying potential safety hazards and safety benefits that may result from planned NAS changes associated with NextGen OIs.

10. See AMS, Section 2.1.4.3, *Standard Lifecycle Work Breakdown Structure*, for more information.

- Address any safety analysis and assessment results in program planning and requirements documents;
- Incorporate any safety issues identified by the SCT or ANG EST into program safety efforts;
- Include any requirements developed as a result of the safety analyses as discrete requirements in the preliminary PRD, the initial PRD, or the final PRD;
- Trace the safety requirements back to identified safety hazards;
- Verify that the mitigations identified to reduce safety risk are included as validated and verified safety requirements in the final SRM document;
- Support the establishment of traceability between safety analysis results and the NAS EA;
- Maintain safety documentation throughout the system lifecycle;
- Include SRM results in investment decision briefings to the JRC; and
- Coordinate the peer review process with the AJI SCLs. (See Section 8.3 for more information on the peer review process.)

4.5.4 AJM Roles and Responsibilities

A designated Group Manager within AJM must:

- Review and approve the following safety documentation during the SI phase:
  - Sub-System Hazard Analysis (see Appendix G).
  - System Hazard Analysis (see Appendix H).
  - Operating and Support Hazard Analysis (see Appendix I).
- Review and accept documentation showing compliance with SAE Aerospace Recommended Practice (ARP)[11] ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*; RTCA[12] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*; and RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware* (or approved alternatives).
- Provide approval of the system before deployment by deciding if the developer has complied with the performance requirements of the contract.

4.5.5 AJI-3 Roles and Responsibilities

As the ATO's focal point for SRM implementation, AJI-3 provides the ATO with safety direction while driving the SRM / Integrated Safety Management process. AJI-3 also coordinates the EA support efforts on the safety roadmap for the ATO.

11. An ARP is a guideline from SAE International.

12. RTCA, Inc., is a private, not-for-profit association founded in 1935 as the Radio Technical Commission for Aeronautics; it is now referred to simply as "RTCA."

AJI-3 must provide safety leadership and expertise to ensure that:

- Operational safety risk in the air traffic services that the ATO provides to the NAS is identified and managed, and
- Safety risk is considered and proactively mitigated in the early development, design, and integration of solutions and across organizations to support NextGen capabilities.

To provide this leadership, AJI-3 must:

- Represent the ATO in resolving high-level safety issues in air traffic operation and decision-making meetings;
- Review and approve certain SRM documentation associated with NAS changes that require AOV approval, as defined in FAA Order 1100.161;
- Review and approve certain SRM documentation for acquisition programs and safety analyses/assessments for changes done at the national level, as defined in the SMS Manual and the SRMGSA;
- Review and approve the following safety input in support of JRC investment decisions and SI, as required:
    - PSP (see Appendix A).
    - Operational Safety Assessment (see Appendix C).
    - Comparative Safety Assessment (see Appendix E).
    - Preliminary Hazard Analysis (see Appendix F).
    - SSAR (see Appendix J).
- Provide final safety approval before a system may be deployed to ensure all system safety requirements have been met;
- Serve as the ATO safety focal point for collaboration with ANG and the PO on NextGen transitional activities;
- Ensure that the safety risk case management process includes Integrated Safety Management to ensure a comprehensive safety review of concepts, solutions, systems, and procedures;
- Provide the Vice President of AJI with senior-level input on ATO safety-related issues for air traffic operations, acquisitions, and Second-Level Engineering changes;
- Review and approve proposed changes to safety policy and guidance for incorporation in FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*, the SMS Manual, and the SRMGSA; and
- Collaborate with internal and external stakeholders to facilitate mitigation of safety risks that cross LOBs.

4.5.5.1 AJI Safety Management Group

The AJI Safety Management Group, AJI-31, provides ATO safety direction, develops and maintains the SRM process, and provides AJI SCLs to facilitate SRM.

4.5.5.2 AJI Safety Engineering Team Manager

The Safety Engineering Team, AJI-314, Manager manages the safety case workload for a team of safety engineers and assigns an AJI SCL to work with an individual program or initiative

based on resource availability. He or she must ensure that SRM documentation is processed in accordance with the SMS Manual, relevant ATO-SG documents, and the SRMGSA before being submitted to AJI-3 for approval and signature.

The AJI-314 Team Manager must:

- Assign an AJI SCL to work with a PO;
- Balance the workload among AJI SCLs to best support the POs considering commonality with existing assignments, their experience and expertise, and program and portfolio complexities; and
- Confirm that any documentation being submitted to AJI-3 for approval has been developed and has undergone peer review in accordance with the SRMGSA and internal AJI processes.

4.5.5.3 AJI SCLs

The AJI SCLs (or their designees) are experts in SRM policy and guidance that pertain to the AMS. The AJI SCLs assist the POs responsible for planning, conducting, or managing system safety. The AJI SCLs are the ATO's acquisition safety focal points and ensure that each safety product requiring AJI-3 signature and associated with an AMS milestone is peer reviewed; they ensure that all resulting comments and concerns are addressed prior to the program's planned AMS decision. The AJI SCLs must:

- Convene SSMs with the POs according to the established milestones and strategy for the development and approval of SRM documentation required to support JRC milestone decisions. This starts in the Concept and Requirements Definition phase and ends during the In-Service Management (ISM) phase.
- Provide safety policy interpretation to the PO when requested.
- At the appropriate time, recommend to the AJI-314 Team Manager that the SRM documentation requiring the AJI-3 Director's signature is ready to enter the peer review process for approval and signatures.
- Lead the peer review of SRM documentation that requires AJI-3 signature (see Section 8.3) within a timeframe that is consistent with the planned JRC decisions.
- Review the PSP to ensure that the proposed processes will be sufficient for generating evidence of compliance with system development assurance standards.
- During the SI phase, periodically review and assess data supplied by the PO to demonstrate that the program has met the safety and system development assurance requirements outlined in the approved PSP.
- Serve on ANG- or SCT-chartered teams as requested to represent the entire ATO from a safety perspective.
- Ensure that safety risk associated with initiatives that have conducted safety analyses/assessments are mapped to and considered in the SRM activities of any acquisition program.
- Document lessons learned that may improve the SRM process.

4.5.5.4 Audits and Assessments

4.5.5.4.1 Audits

AJI-3 provides the ATO with mechanisms to ensure the safety of the NAS by identifying areas of risk or concern. AJI-3 uses a streamlined process to audit requirement compliance and potential safety risk and to assess the effectiveness of mitigation strategies. AJI-3 may audit the PO's implementation of system safety and system development assurance to determine their compliance with requirements outlined in the approved PSP or other planning documentation and to support AJI-3's signing of the SSAR.

4.5.5.4.2 Assessments

The Independent Safety Assessments Team, AJI-315, is responsible for evaluating designated acquisition systems (and major modifications) through the Independent Operational Assessment (IOA) function.[13] To ensure that solutions are within acceptable levels of safety risk, the SMS and AMS require that IOAs be conducted on designated systems prior to the deployment decisions (such as the In-Service Decision (ISD)) to identify safety hazards and operational concerns in a representative operational environment. This team also uses a structured process to assess the safety and operational readiness of new systems prior to deployment in the NAS.

During the ISM phase, AJI-315 is also responsible for conducting post-implementation safety assessments of designated systems, procedures, and service capabilities to independently assess the residual risk of changes in the NAS, identify any new hazards or operational concerns not anticipated during SRM, and ensure the mitigations for identified hazards have been properly implemented and comply with SMS requirements.

If new safety hazards are identified through an Independent Safety Assessment, the PO (working with the AJI SCL) may have to reconvene SRM panels to analyze and assess these hazards.

4.5.5.5 ISD Executive Secretariat

The ISD Executive Secretariat facilitates the AMS policy for deployment planning and the In-Service Review (ISR); prepares records of decisions and ISD closeout memoranda; and supports POs in their efforts to adhere to AMS policy, complete the ISR checklist, satisfy the ISD entrance criteria, compile an ISD briefing, and provide monthly updates after the ISD. All POs seeking a JRC Final Investment Decision, regardless of acquisition category level, must coordinate with the ISD Executive Secretariat.

13. See AMS, Section 4.5, *Independent Operational Assessment*, for more information.

5 Safety Planning for Acquisitions

5.1 Safety Strategy Meetings and Program Safety Plans

Acquisition strategies vary among investment programs. As a result, the Safety Risk Management (SRM) documentation requirements may also vary. Early in the SRM effort, the Program Office (PO) must contact Safety and Technical Training (AJI) to schedule a Safety Strategy Meeting (SSM) to determine the appropriate documentation requirements and to understand the PO's SRM obligations for anticipated Federal Aviation Administration (FAA) Acquisition Management System (AMS) milestones. The PO must submit a Safety Strategy Worksheet (SSW)[1] to the AJI Safety Case Lead (SCL) prior to the SSM. The AJI SCL must facilitate the SSM, clarify, if necessary, any policies and SRM practices, and establish peer review process guidelines. The AJI SCL must capture the SSM proceedings and any agreements made in meeting minutes that document the strategy agreed upon by attendees to satisfy acquisition SRM and system development assurance requirements. The AJI SCL should consult with AJI management as necessary (particularly if extensive documentation tailoring is planned).

The SSM can be held at any time per the request of the PO from project inception through the fielding of the system (including prior to the Initial Operating Capability being declared). However, to gain the maximum benefit for the program, the SSM must occur early enough in the process to schedule SRM documentation development, review, coordination, and necessary approvals prior to the PO's next investment milestone decision point. SRM is a required checklist item for the Investment Analysis Readiness Decision (IARD), the Initial Investment Decision (IID), the Final Investment Decision, and the In-Service Decision.

The Office of the NextGen (ANG) Enterprise Safety and Information Security Division, ANG-B3, must be invited to participate in all SSMs. For SSMs held for programs in or about to enter the Concept and Requirements Definition (CRD) phase, the POs must consult with the ANG CRD lead before the SSM convenes.

At the SSM, the PO and the AJI SCL must discuss what SRM / system development assurance documentation is required and the timing of the AJI-led peer review of any PO-submitted safety documentation that requires the approval of the Director of Policy and Performance, AJI-3. Similarly, the PO and the AJI SCL must discuss the timing of any PO-led peer reviews of safety and system development assurance documentation that requires the approval of the Program Management Organization. The PO and the AJI SCL must agree to a firm timeline of comment submittals and adjudications and commit to following a prescribed schedule. This schedule must be documented in the SSM minutes and included in the Program Safety Plan (PSP). The PO and SCL must also discuss the compliance data that will be submitted during the solution implementation phase.

Sometimes, acquisition strategies change or there is not enough information available to determine the SRM documentation requirements for the entire acquisition lifecycle. If so, additional SSMs may be scheduled as often as necessary.

The SSM minutes form the basis of the PSP, which sets the overall safety strategy for the program when approved. The PO must develop the PSP and receive approval from the AJI-3 Director prior to developing any other SRM documentation (except in the case of a baseline change). A PSP must be approved before the IARD, if feasible, but no later than the IID. The

1. Contact the AJI Safety Case Lead for the latest version of the SSW.

PSP defines which SRM and system development assurance processes must be conducted during a system acquisition and which safety requirements must be fulfilled before system deployment. If documented in an approved PSP, the PO may use alternative methods other than those described in the Safety Risk Management Guidance for System Acquisitions' appendices to capture required information. Also, if documented in an approved PSP, the PO may prepare a combined analysis (e.g., a combined System Hazard Analysis / Sub-System Hazard Analysis) or bypass analyses entirely to meet AMS policy requirements. The PSP must be updated as necessary as the program proceeds through its acquisition lifecycle.

5.1.1 Consistency with the Implementation Strategy and Planning Document

As stated in Sections 2.3.3.1.4 and 2.3.4.1.5, the PO is responsible for preparing an Implementation Strategy and Planning Document (ISPD). Section 7.1 of the ISPD specifically addresses the program's system safety plans. This section must be approved by the AJI-3 Director. At the SSM, the AJI SCL must work with the PO to ensure that the safety strategy that is or will be delineated in the ISPD is consistent with that in the PSP.

5.1.2 Technology Refreshment Portfolio

For a Technology Refreshment (TR) portfolio, the TR Portfolio Manager must contact the AJI SCL and conduct an SSM prior to developing the portfolio PSP to assist in tailoring any safety documentation requirements. It is possible that the complexity of some sub–Acquisition Category (ACAT) 1 TR projects may warrant the development of project-specific PSPs to supplement the portfolio PSP; this need must be detailed in the approved portfolio PSP. There is no need to develop project-specific PSPs for sub-ACAT 2 TR projects because the portfolio PSP would outline the SRM and development assurance requirements for these projects.

6 Other Considerations

6.1 Baseline Change Management

For any acquisition program under its jurisdiction, the Joint Resources Council (JRC) approves and baselines all Federal Aviation Administration (FAA) program documents required by the FAA Acquisition Management System (AMS) (i.e., Program Requirements Documents (PRDs), acquisition program baselines, Business Cases, and Implementation Strategy and Planning Documents). The JRC may also make acquisition program baseline change decisions that alter program performance or cost and schedule baselines during the Solution Implementation phase for investment programs. From a Safety Risk Management (SRM) viewpoint, if a baseline change is being proposed, the Program Office (PO) must review and update the Program Safety Plan (PSP) and any safety analyses/assessments that have already been completed, as necessary, to ensure that the new baseline does not impact the risk mitigation strategies already identified. If the proposed change does affect safety risk mitigation strategies, then the predicted residual risk identified in the completed safety analyses/assessments may not be achievable, and the new predicted residual risk without these mitigations implemented may be unacceptable.

A baseline change could affect already identified risk mitigation strategies in the following ways:

- If the program cost is being re-baselined, the proposed new budget may not include funding to implement the mitigations previously identified;
- If the schedule is being re-baselined, the proposed new schedule may impact the temporal aspects of the identified risk mitigation strategy (i.e., the planned mitigations may not be in place as expected and required); or
- If the performance is being re-baselined, the new requirements may be sufficiently different from the assumptions made and analyses conducted as part of previous safety assessments may no longer apply, invalidating previously identified risk mitigation strategies.

6.2 Program Safety Requirements for Decommissioning and Disposal

Disposal of an asset or program is part of the In-Service Management phase of the AMS process and, as such, requires SRM as part of its lifecycle management.[1] In addition, decommissioning a service provided by a program asset targeted for disposal could occur much earlier than the actual disposal and must also meet all SRM requirements. Programs or assets facing disposal often have their SRM requirements met by the program or asset replacing them, but this is not always the case.[2] Prior to the decommissioning and/or disposal of an asset or program, the associated PO must contact the Safety and Technical Training (AJI) Safety Case Lead (SCL) to convene a Safety Strategy Meeting (SSM) to determine whether SRM analysis and subsequent SRM documents are required. If so, an SRM panel must perform an analysis/assessment, similar to a Preliminary Hazard Analysis (PHA), to identify safety hazards associated with the disposal activity. This may include deactivation, deactivation and replacement of the system, or similar considerations.

1. Decommissioning and disposal must also follow the media sanitization requirements in FAA Order 1370.121, *FAA Information Security and Privacy Program & Policy*.

2. The following can be assumed: (1) once a National Airspace System (NAS) asset is removed from service, it is no longer part of the flight-day decision-making process, and (2) even if a NAS asset remains in an operational area in a deactivated state, removal and disposal may occur without regard to aircraft movement. However, SRM is a data-driven process (i.e., a process not driven by opinion) that still must be conducted.

6.3 Site Implementation

FAA Order JO 6000.50, *National Airspace System (NAS) Integrated Risk Management*, complements existing policies regarding SRM and standardizes processes for Operational Risk Management (ORM) during installation activities. FAA Order 6000.15, *General Maintenance Handbook for National Airspace System (NAS) Facilities*, defines ORM and clarifies both SRM and ORM policy to assist field managers with risk management activities during installation actions. ORM/SRM integration addresses three distinct categories of effort:

- Implementation activities,
- Modifications, and
- Required maintenance.

Per FAA Order JO 6000.50, the PO must prepare a Generic Site Implementation Plan (GSIP), conduct SRM, and prepare an SRM document on the GSIP itself. A GSIP is required for all construction, installation, and/or removal activities in the National Airspace System (NAS). The GSIP contains an SRM section that provides installers and maintainers with any identified hazards, mitigations, and residual risk identified during the acquisition process, as documented in the System Safety Assessment Report (SSAR) and as applicable. Note that operational risks may have no impact on safety but must be considered before a system is deployed.

6.4 Legacy System SRM

Often, acquisitions support changes to legacy systems. These changes can either result in systems that are functionally identical to the original system or systems that can add to or improve existing functionality. In all cases, the PO must analyze the change to determine whether it introduces/reveals any new hazards or affects the safety risk level of the operation/system.

A change to a legacy system that is initiated due to component obsolescence may include a Technology Refreshment (TR), Service Life Extension Programs, Replacement-in-Kind Programs, Facility Initiative Programs,[5] and Variable Quantity Programs.[6] It has been commonly accepted that a change that results in a "box-for-box" replacement of obsolete or unserviceable components containing identical functionality (i.e., a form, fit, and function replacement) has no impact on NAS safety. However, lessons learned have shown that new hazards may be introduced if a more technically sophisticated multi-component system attribute "box" is being installed to replace a "box" that achieves the same function. If this is the case, the full SRM process must be followed. If the change does not introduce/reveal any new hazards or affect the existing safety risk level of the operation/system, then this result may be documented in an SRM document without hazards. The supporting documentation must justify this decision. Refer to the Air Traffic Organization (ATO) Safety Management System (SMS) Manual for SRM document requirements.

Changes to legacy systems can involve the addition of new functions or the introduction of a new combination of existing functions to the legacy system. New technologies may also have an effect on existing hazards or how they are controlled. For example, a particular function may be activated by a mechanical switch in the legacy system but enabled by software in the legacy system's changes. If the analysis of the changes determines that there are new or newly

5. A Facility Initiative Program is a program associated with the new construction, replacement, modernization, repair, remediation, lease, or disposal of the FAA's manned and unmanned facility infrastructures.

6. A Variable Quantity Program is a program that includes insertions, modernizations, or additions to quantities of systems or subcomponents previously fielded and in operation within the FAA.

combined functions, or if there is any impact on existing hazards or how they are controlled (or any introduction of new hazards), the standard SRM activities documented in the SMS Manual are required.

These analyses may be facilitated by examination of the legacy system's Concept of Operations, Functional Analysis, Shortfall Analysis, Enterprise Architecture products, and preliminary requirements in the preliminary PRD, if any exist. Most likely, detailed design and "as-built" technical baseline documentation with successive modifications are sufficient for lifecycle support, yet they may lack in early explanations of the concepts, alternatives, and requirements that the legacy system traded off years ago. Years of live operational data archives may be present, which must be valued more highly than plans, models, or future expectations of performance. For example, many years of adequate specification performance to a frozen baseline at multiple sites (actuals) must trump independent, discontinuous future estimates of failure likelihood that ignore such a strong basis for trend analysis. In all cases, the PO should hold an SSM with the AJI SCL to determine if the program should develop an SRM document per the current AMS milestone requirements.

A program undergoing legacy system changes needs to comply with all aspects of the AMS and SRM processes. The requirements for each legacy system change are typically very streamlined or tailored compared to the original program. Each legacy system change varies in its purpose and requirements, but the SRM requirements may be minimal if the legacy system change's form, fit, and function are the same as when the program first went through the AMS process.

6.5 Physical Security, Information Security, Cybersecurity, and Occupational Safety and Health

Physical security, information security,[7] cybersecurity, and Occupational Safety and Health (OSH) (including Fire Life Safety (FLS)) issues can sometimes affect the safety of the operational NAS. When this is the case, these issues fall within the scope of the SMS. The PO must consider these issues and record them in the SRM document as well as treat, track, and monitor them as safety requirements in accordance with the processes contained in the SMS Manual. Consideration of such issues is best done by consulting representatives from each discipline prior to convening any SRM panel and allowing their participation in the SRM panel, as necessary.

6.5.1 Safety and Security Issue Reporting

Regardless of whether an issue falls within the scope of the SMS, the PO is responsible for reporting any potential OSH, information security, operational security, physical security, and cybersecurity issues identified by an SRM panel to the appropriate authority for possible mitigation. Such issues must also be recorded in the SRM document. The appropriate authority for most security issues is System Operations Services (AJR) ATO Security, AJR-2. OSH issues (including FLS) should be reported to the appropriate Service Area's OSH/FLS professional or to Environmental and OSH Services headquarters.

6.6 Commercial Off-the-Shelf Products

Using a Commercial Off-the-Shelf (COTS) product, even if it has very high reliability, does not imply that the product is safe when it interacts with other system components. Problems could be exacerbated by software because software usually controls many, if not all, of the interactions between system components. Techniques for dealing with COTS by simply equating software reliability or correctness (consistency with specifications) with safety may not

7. FAA Order 1370.121, in conjunction with the FAA Cybersecurity Steering Committee, applies.

prevent system accidents. In many cases, using COTS components in safety-critical systems with acceptable risk may simply be infeasible. In these cases, it is safer and less expensive to provide special-purpose software; using COTS amounts to false economy that costs more in the end.

There are, however, situations in which COTS components can be assured to have adequate system safety. In these cases, either the system design must allow protection against any possible hazardous software behavior or a complete "black box" behavior specification must be provided by the producer of that component in order to perform a hazard analysis.

6.7 Safety Performance Targets and Monitoring Plans

All safety requirements must be verified and validated as the system is developed, prior to implementation. In a typical acquisition program, the PO must accomplish this by applying development assurance methods and conducting design audits, developmental and operational tests and evaluations, and/or performance checks.

However, the verification and validation of safety requirements does not eliminate the need for monitoring the safety performance of the eventual fielded system. Monitoring of PHA-level hazards must be performed on an operational system; the phrase "verified in test" must not be used in a monitoring plan.

The PO must establish safety performance targets for all medium- and high-risk hazards that were initially identified in the PHA; all medium- and high-risk hazards that were subsequently identified in the System Hazard Analysis (SHA), Sub-System Hazard Analysis (SSHA), or Operating and Support Hazard Analysis (O&SHA) and could not be traced back to PHA-identified hazards; and all predicted residual medium-risk hazards. The PO must develop an operational monitoring plan to track these performance targets.

The duration of the monitoring activities depends on the complexity of the system being deployed, the sites at which the system will be deployed, and the nature of the established safety performance targets. The guidelines for determining monitoring activity duration are described below.

- Monitoring activities may continue until the capability/requirements related to the hazard have been implemented or are operational (i.e., are in use) at one or more facilities beyond the key site(s).
- Monitoring activities may continue for at least one year and must be developed for each phase of a segmented or phased deployment of a system; additional monitoring activities must be conducted for TR and software enhancement acquisition programs.
- Monitoring activities may conclude three months after the target facility is operational (i.e., after the target facility has been commissioned or after the operational readiness declaration).
- Monitoring activities may be conducted, at a minimum, quarterly for initial high-risk hazards and twice a year for initially identified or predicted residual medium-risk hazards.

The AJI SCL may recommend additional or tailored monitoring activities based on a particular system, the deployment activities, and/or the nature of the safety performance targets if they differ significantly from a traditional acquisition.

Monitoring plan developers and reviewers must ensure PHA-level safety requirements (as well as the lower-level SHA, SSHA, and O&SHA safety requirements that trace back to the PHA-level safety requirements) are addressed in the SSAR and tabulated in the Safety Requirements Verification Table. The PHA and the SSAR must be updated if requirements change after implementation or if new safety hazards are identified from safety assurance findings (i.e., an Independent Operational Assessment (IOA)). The risk acceptor or his or her designee must conduct the monitoring.

The PO may need to develop additional or modified post-deployment monitoring plans as part of the SRM effort if either of the following conditions apply:

- The SSAR identifies workarounds to safety requirements that were not implemented prior to initial deployment despite the In-Service Decision Authority granting approval to deploy, or
- Additional safety requirements are developed post–Initial Operational Capability because of Operational Suitability Demonstrations, IOAs, or Post-Implementation Reviews.

Refer to the SMS Manual or contact the AJI SCL for more information on safety performance targets and monitoring plans.

6.8 Program Segmentation

If an acquisition program is released in segments over time, each segment may require its own PSP that references the versions of the SMS Manual and Safety Risk Management Guidance for System Acquisitions (SRMGSA) that are current at the time the PSP is approved. In addition, if safety hazards identified in a previous segment have been successfully mitigated to an acceptable safety level prior to a subsequent segment (i.e., the mitigation met the monitoring plan requirements), then that mitigation becomes an existing control for subsequent segments. The safety analyses of subsequent segments should start at the new safety baseline of the previous segment.

6.9 Program Risk Management

The PO must apply program risk management throughout the AMS lifecycle management process to identify and mitigate risks associated with achieving FAA goals and objectives. Each investment program should institute risk management processes in accordance with AMS policy and guidance. The FAA's policy related to risk management can be found in AMS, Section 4.13, *Risk Management*.

Program risk management and SRM have separate foci; for instance, cost and schedule impacts are not factored into a safety assessment but are part of program risk management. However, program risk management and SRM are not mutually exclusive. Safety risk that is not properly mitigated can become a program risk by delaying or stopping the implementation of activities and, consequentially, affecting program cost or schedule. Knowledge of SMS policies and proper planning help the PO minimize any SRM impacts to cost and schedule. AJI SCLs can also assist in this area.

7 Alternative Processes

Every program is different in scope, complexity, criticality, and resources. In recognition of these differences, Program Offices may use alternative processes when performing Safety Risk Management (SRM) or system development assurance when the standard means of compliance cannot be achieved and there is no impact to the National Airspace System of not using the standard means of compliance.

7.1 Alternative SRM Process

An alternative SRM process may be used under the following conditions:

- The alternative process must meet the minimum requirements outlined in the Air Traffic Organization Safety Management System Manual.
- The use of alternatives (e.g., SAE Aerospace Recommended Practice (ARP)[1] ARP4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*) must be discussed at the Safety Strategy Meeting (SSM); agreed to by the Safety and Technical Training (AJI) Safety Case Lead (SCL); and documented in the meeting minutes.
- The alternative process must be described in an approved Program Safety Plan (PSP).

7.2 Alternative System Development Assurance

Alternative system development assurance processes may be used under the following conditions:

- The use of alternative processes must be justified with a gap analysis showing that it meets the objectives of ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*; RTCA[2] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*; or RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*, as applicable.
- The use of alternative processes must be discussed at the SSM, agreed to by the AJI SCL, and documented in the meeting minutes.
- The alternative process must be described in an approved PSP.

1. An ARP is a guideline from SAE International.

2. RTCA, Inc., is a private, not-for-profit association founded in 1935 as the Radio Technical Commission for Aeronautics; it is now referred to simply as “RTCA.”

8 Safety Risk Management Documentation, Approval, and Tracking

8.1 Safety Risk Management Documents

For an acquisition, the Safety Risk Management (SRM) process is a series of analyses/assessments that starts at the Operational Safety Assessment (OSA) and continues through the Comparative Safety Assessment (CSA), the Preliminary Hazard Analysis (PHA), the Sub-System Hazard Analysis (SSHA), the System Hazard Analysis (SHA), the Operating and Support Hazard Analysis (O&SHA), and the System Safety Assessment Report (SSAR). Not all of these analyses/assessments are required for every program. To determine the specific safety analyses/assessments required for a particular program, the Program Office (PO) and the Safety and Technical Training (AJI) Safety Case Lead (SCL) must hold a Safety Strategy Meeting; the PO must document the agreements made at this meeting in a Program Safety Plan (PSP). The PSP, when approved, becomes part of the SRM documentation. Each analysis/assessment becomes more discrete as more design details are known and as the product moves through the Federal Aviation Administration (FAA) Acquisition Management System (AMS) lifecycle. The PO must maintain all SRM documents in the Safety Management Tracking System (SMTS) as a record of the project's progress.

The basis of each analysis is a Hazard Analysis Worksheet (HAW).[1] The HAW, initially developed early in the system lifecycle while conducting a PHA, is further developed, modified, and enhanced as subsequent analyses are conducted. Each subsequent analysis has a slightly different focus but is essentially a HAW that builds on the previously developed HAW.

If an SRM panel finds that a change to an **existing** system will not introduce new hazards or increase safety risk in the National Airspace System (NAS), then there is no need to conduct further safety analyses/assessments. The PO must ensure the SRM panel's safety finding without hazards, along with the justification as to why the change is not subject to additional SRM analyses/assessments, is documented in an SRM document.

This SRM document must also include a:

- Description of the NAS change and affected hardware; software; and/or operational NAS equipment, operations, and/or procedures; and
- Justification for the determination that there are no new hazards or any expected changes to the current risk associated with the implementation of the NAS change.

8.2 Mission Support Programs

When an acquisition has an effect on the safety of the NAS, the PO must conduct and document the SRM process throughout the lifecycle of the product or service in accordance with Air Traffic Organization (ATO) Safety Management System (SMS) policy. The PO must contact the Safety Engineering Team, AJI-314, Manager, to initiate discussions if they believe their program is exempt from SRM requirements. In the ATO, Policy and Performance, AJI-3 has been designated as the office responsible for determining whether an acquisition requires SRM. After consultation with the PO, if AJI-3, determines that a mission support program does not require SRM, then AJI-3 must provide documented notification to the Joint Resources Council (JRC) Executive Secretariat accordingly. If it is determined that SRM is required for a mission support program, then the PO must conduct the program in accordance with

1. The components of a HAW are detailed in the Air Traffic Organization Safety Management System Manual.

appropriate requirements in the ATO SMS Manual / Safety Risk Management Guidance for System Acquisitions (SRMGSA).

8.3 Peer Review Process

An SRM document peer review is an independent review to determine whether the SRM document meets SMS policy and FAA safety objectives. Peer reviewers must objectively review the document to ensure the analysis/assessment is accurate and operationally sound (i.e., the safety hazards, causes, effects, and safety requirements are appropriate).

All SRM documents requiring AJI-3 approval (i.e., PSPs, OSAs, CSAs, PHAs, and SSARs) must undergo an AJI-led peer review prior to the signature cycle. The PO / safety representative must submit each completed SRM document to the AJI-314 general mailbox (9-awa-aji-3000@faa.gov) and courtesy copy his/her assigned AJI SCL in preparation for peer review. The AJI SCL must first review the SRM document to determine its compliance with the operative SMS Manual and the SRMGSA. If the AJI SCL determines that the SRM document is not ready to proceed to peer review, then he/she must return it to the originator with recommendations for resolution.

Following the AJI SCL's preliminary review of the SRM document to ensure the document follows AJI policy, the AJI SCL must distribute the SRM document for peer review and comments. After comments are received and collated, the SCL must screen the comments for technical merit and modify or eliminate any comments that are inappropriate. Then, the AJI SCL must work with the PO / safety representative to adjudicate the comments and generate written responses to the commenters. (If the AJI SCL and the PO cannot agree on a proposed adjudication, the issue must be raised to the AJI-314 Team Manager for discussion and resolution.) The commenters must review the responses and/or changes to the document for concurrence. If a commenter submits partial concurrence or non-concurrence to a response, this must be mediated via discussions involving the commenter, AJI SCL, and PO / safety representative. If comments cannot be resolved to the commenter's satisfaction, then the AJI SCL must elevate the commenter's concerns to the AJI-314 Team Manager for discussion and resolution. Once all of the comments are resolved, the AJI SCL must provide a final compilation of all comments and their dispositions to all peer reviewers. The PO / safety representative must update the SRM document in accordance with the adjudicated comments.

Figure 8.1 shows a high-level flow diagram of the AJI document review process, of which the peer review process is a subset. The duration dates shown are suggested but not mandatory dates for each action. The general peer review timeline is dependent upon various factors including, but not limited to:

- The complexity of the safety analysis/assessment,
- The number of stakeholders involved,
- The complexity of new technologies and interfaces,
- The effectiveness of any reviews previously conducted, and
- Projected JRC decision dates.

The PO / safety representative must negotiate with the AJI SCL for firm review dates, if possible, during the initial document submittal process. These dates should be included in an approved PSP.

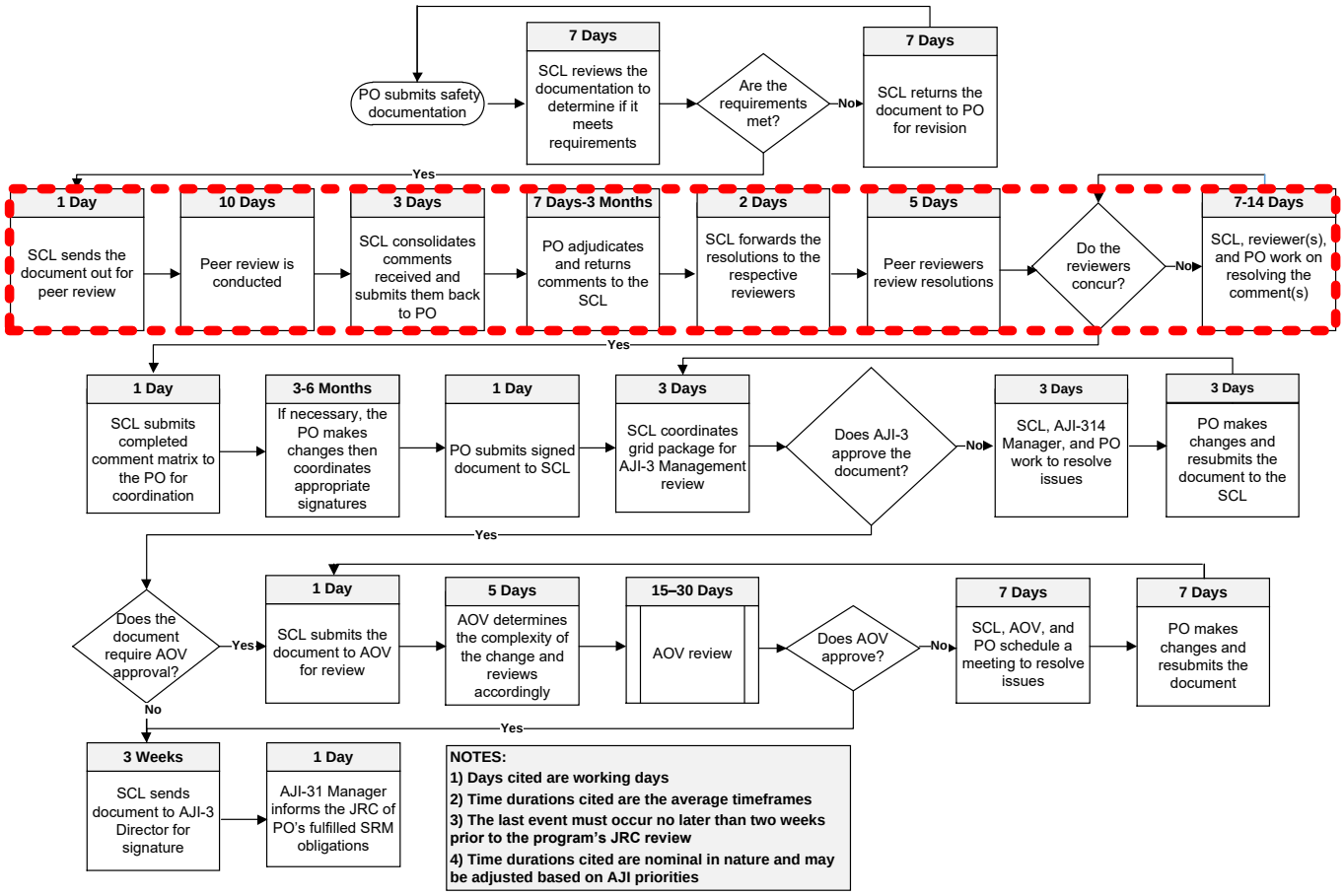

Figure 8.1: Document Review Process Flow

AJI-3 has strategically identified and designated peer reviewers from various organizations across the ATO and the Office of NextGen (ANG) to support the independent peer review process. Organizations represented in the peer review must include:

- Safety Policy Team, AJI-311;
- Safety Engineering Team, AJI-314;
- Independent Safety Assessments Team, AJI-315; and
- Enterprise Safety and Information Security, ANG-B3.

If applicable, the AJI SCL may ask other organizations/subject matter experts to participate in the peer review, including:

- Quality Control Group representatives from the Service Center;
- Air Traffic Safety Oversight Service (AOV) Air Traffic Safety Standards Oversight, AOV-100, representatives;
- Human factors Subject Matter Experts (SMEs);
- Environmental and Occupational Safety and Health Services representatives;

- Cybersecurity SMEs; and
- Representatives from other ATO offices.

Per Section 2.2.2, the PO must review and maintain final approval of the following safety deliverables as required by the system developer's contract: the SHA, the SSHA, and the O&SHA. Additionally, each PO must review and approve SAE Aerospace Recommended Practice (ARP)[2] ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*; RTCA[3] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*; and RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*, or other development assurance deliverables as required by the contract. The PO must consider any AJI SCL's review and comments prior to the PO's final concurrence and acceptance of any safety deliverables. The PO must also ensure that the safety deliverable is peer reviewed by appropriate subject matter experts. After the general peer review process is completed and all comments are adjudicated, the safety deliverable may be finalized, approved, signed, and accepted in accordance with Program Management Organization operating procedures and the applicable Statement of Work and/or contract.

8.4 Approval Authorities and Coordination Requirements

The SMS Manual contains the guidance and coordination requirements for the review, approval, and risk acceptance of SRM documentation contained completely within a Service Unit (SU), across multiple SUs, or across multiple lines of business. SRM documentation must not be submitted to AJI-3 Director for approval until it has undergone the AJI peer review process. The AJI-3 Director is also the approval authority for PSPs as well as the representative that informs the JRC and In-Service Decision Executive Secretariat's groups which programs are compliant with SMS requirements.

8.5 SMTS

SMTS is the official repository for all completed ATO SRM documents. The PO must use SMTS for all safety analyses/assessments beginning with the OSA and continuing throughout the product's lifecycle. Its primary purpose is to track hazards and their mitigations. SMTS houses SRM documents and their associated safety analyses/assessments, allowing change proponents and SRM panels to use this information for similar efforts. Additionally, SMTS tracks implementation and ongoing monitoring activities, which enables risk acceptors to assess and track predicted residual risk.

The following details are required in SMTS:

- Project title (this must be the same program name used for JRC purposes);
- Safety analysis/assessment type (i.e., OSA, CSA, PHA, SHA, SSHA, O&SHA, or SSAR);
- Organization name;
- Organization description (this must be the name of the responsible PO);
- Safety analysis/assessment title;

2. An ARP is a guideline from SAE International.

3. RTCA, Inc. is a private, not-for-profit association founded in 1935 as the Radio Technical Commission for Aeronautics; it is now referred to simply as "RTCA."

- Whether the AJI-3 Director's signature is required;
- Whether issues/hazards were identified;
- A HAW for each identified hazard (this must include a hazard ID and hazard description and must be done by the time of implementation (i.e., as part of the SSAR));
- Uploaded copies of approved PSPs; and
- Uploaded copies of the final, approved, and signed safety analyses/assessments (i.e., OSA, CSA, PHA, SHA, SSHA, O&SHA, SSAR, or other).

Note: If a Program Requirements Document (PRD) is being used in lieu of providing signatures for safety requirements, then a copy of the signed/approved PRD must be uploaded to SMTS.

Any SRM documents must be approved by the AJI-3 Director or the PO, as applicable, before an acquisition milestone / decision point. The PO must record SRM document activity and information in SMTS prior to that milestone / decision point or within 30 days after document approval (whichever occurs first).

9 System Safety Considerations

9.1 System Safety

For each new and modified system acquisition and development, system safety is a standardized management and engineering discipline that integrates the consideration of human, machine, and environment in planning; designing; testing; and maintaining operations, procedures, and acquisition projects. System safety is applied throughout a system's lifecycle to achieve an acceptable level of safety risk within the constraints of operational effectiveness, time, and cost. As part of the system safety process, all safety requirements (including Development Assurance Levels (DALs)) must be revisited and modified as necessary as development gets more discrete.

For each new and modified system acquisition, the Program Office (PO) must establish and implement system safety practices, including system development assurance, to meet the requirements of the Air Traffic Organization (ATO) Safety Management System (SMS). The status of system safety must be presented at all decision points and investment reviews. Detailed guidelines for safety management and development assurance are found on the Federal Aviation Administration (FAA) Acquisition System Toolset (FAST) website; in the ATO SMS Manual; and in SAE Aerospace Recommended Practice (ARP)[1] ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*; in RTCA[2] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*; and RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*.

Section 5.4 of the preliminary Program Requirements Document constitutes the high-level safety plan required by the Safety Risk Management Guidance for System Acquisitions for the Investment Analysis Readiness Decision (IARD). The PO must develop a more specific Program Safety Plan (PSP) consistent with this safety plan for the IARD and update it for the Initial Investment Decision and Final Investment Decision. The PSP's scope, content, and list of required Safety Risk Management (SRM) activities are based on the Safety Strategy Meeting that must be conducted between the PO and the Safety and Technical Training (AJI) Safety Engineering Team, AJI-314. See Appendix A for more information concerning PSPs.

9.2 Integrated Safety Management

The PO must perform Integrated Safety Management to assess the risk of initiatives in support of agency Risk-Based Decision Making. The legacy National Airspace System (NAS) is a "system of systems" that provides multiple services to users. The NAS—and in particular, the Next Generation Air Transportation System (NextGen)—is evolving into an even more complex configuration that is highly distributed and interconnected. Future acquisitions are beginning to blur the lines of what is considered a "system" with defined/fixed boundaries and interfaces. Systems, programs, and projects no longer have unique or exclusive functionality. In fact, the functionalities not only overlap, but may also build on one another, subsume each other, or combine for a joint function or capability. This perspective was not considered historically but is important to applying the concept of integrated safety in acquisitions.

Integrated Safety Management represents a more robust, holistic, and integrated approach to performing safety analyses. It uses existing safety policy and methodologies as well as systems

1. An ARP is a guideline from SAE International.

2. RTCA, Inc., is a private, not-for-profit association founded in 1935 as the Radio Technical Commission for Aeronautics; it is now referred to simply as "RTCA."

engineering processes. It is a critical component not only for successfully achieving the NextGen vision, but also for implementing all enhancements to the NAS.

Directionality is a critical aspect of Integrated Safety Management. Safety assessments using Integrated Safety Management principles must be conducted in three "directions":

- **Vertical integration** ensures the consistency of safety assessments across hierarchical levels from the program or system-level up to the NAS-level. It is essentially a look "up" the NAS at enterprise-level/project-level architectural alignment.
- **Horizontal integration** ensures that the interactions and interdependencies across organizations, operational capabilities, portfolios, operational improvements, increments, current operations, and individual programs or systems are addressed in safety assessments. It is essentially a look "across" the NAS at project-level, inter-architectural alignment, linkages, and interdependencies.
- **Temporal integration** ensures that the impacts of hazards and their associated mitigations across implementation timelines are understood and taken into consideration. It is a look at the impact of phased implementations of NAS initiatives.

Identifying hazards and assessing safety risk remains the basis of all safety management efforts for FAA programs. Integrated Safety Management does not change the basic SRM process; it expands the perspective of the required analysis/assessment and uses existing elements of the FAA's systems engineering process to ensure that no safety gaps occur as aviation capabilities are developed and implemented in the NAS.

9.3 FAA / System Developer Interface

The PO is responsible for conducting a robust system safety effort for any ongoing system development, which entails conducting and approving some required safety analyses. However, due to the technical nature of most systems, the FAA typically cannot conduct such an effort without extensive coordination/cooperation with the system developer during the Solution Implementation phase. Details of this coordination/cooperation must be clearly defined in the Statement of Work (SOW) contained in the contract between the FAA and the system developer. The SOW should be supplemented by Data Item Descriptions (DIDs). (Note: DIDs are available on the FAST website. The PO may tailor any DID to reflect the requirements of a particular program.)

Consider the following while developing contractual requirements for a system safety effort:

- System safety is a basic requirement of the total system. The results of the system safety effort depend on the PO's clear communication of objectives/requirements in the SOW.
- System safety requirements are basic tools for systemically developing design specifications.
- System safety must be planned as an integrated and comprehensive safety engineering effort that is sequential and continual.
    - The system developer's System Safety Program Plan (SSPP) must align with the PO's PSP.

- The timing of safety analyses must be consistent with the engineering milestones outlined in the FAA Systems Engineering Manual.

- Any SRM panel facilitated or conducted by the system developer (i.e., for a Sub-System Hazard Analysis or System Hazard Analysis) must include Subject Matter Experts (SMEs), particularly those who can provide input from an operational perspective.
- The FAA must actively review and be able to modify/comment on the safety analysis documentation as the system developer is preparing it and not just after its final delivery.

9.4 System Development Assurance

System development assurance is the use of a systematic approach to prevent errors from being incorporated into the design, be it at the enterprise, system, architecture, electronic hardware, or software level. For each new and modified system acquisition, the PO must establish a system development assurance program that is compliant with the objectives of the following standards:

- SAE ARP4754A;
- RTCA DO-278A; and
- RTCA DO-254.

System development assurance extends throughout the entire product lifecycle.

9.4.1 Determining the System DALs

System development assurance is performed to determine the proper level of rigor to be applied during design, development, and testing for the system, software, and electronic hardware activities. An appropriate level of rigor is necessary to ensure confidence that the component does not cause or contribute to a system hazard. Determining the system-level Functional DALs (FDALs) related to the most severe hazard and electronic hardware and software items is a five-step process:

1. Determine the associated system functions and their purpose within the system.
2. Determine associated hazard severity classifications based on worst-credible effects of the hazards identified within the system. Refer to the severity classifications defined in the SMS Manual for guidance. Note: Severity is based on the effects to the aircraft and not on Air Traffic Control workload.
3. Assign the FDAL in accordance with the hazard's severity classification within a given function. Note*:* The FDAL is based on the highest hazard severity within each function of the system.
4. Determine whether architectural considerations warrant an FDAL different from the initial FDAL assigned to each function. In some cases, architectural mitigation may justify a revision of the FDAL to a less stringent classification. Guidance for architectural mitigation may be found in SAE ARP4754A.
5. Allocate the system-level FDALs to the associated software and electronic hardware items within the system architecture as Item DALs (IDALs).

The FDALs and IDALs are the mitigations that prevent the hazard of a development error. Compliance to FDALs/IDALs is a safety requirement that must be identified in the SRM document in order for it to be properly tracked and eventually verified and validated.

9.5 Conducting a Compliance Gap Analysis

Many of the non-airborne CNS/ATM systems have been developed and fielded using system, software, and electronic hardware development processes other than those in SAE ARP4754A, RTCA DO-278A, and RTCA DO-254, such as those contained in Institute of Electrical and Electronic Engineers Standard 12207, *Systems and Software Engineering – Software Life Cycle*, or in the vendor's best practices. This could potentially result in problems when incorporating system development assurance requirements for additions to and/or modifications of noncompliant legacy systems. For these cases, a compliance gap analysis must be used to evaluate how the noncompliant processes adhere to SAE ARP4754A, RTCA DO-278A, and RTCA DO-254 processes.

The PO must conduct a compliance gap analysis for each noncompliant system/software/electronic hardware development assurance process being evaluated. The compliance gap analysis provides a basis for addressing any shortfalls from the preferred SAE ARP4754A, RTCA DO-278A, and RTCA DO-254 objectives and guidance. The gap analysis compares existing processes with these processes and identifies deficiencies. It is used not only to identify compliance gaps, but also to define plans for resolving deficiencies.

SAE ARP4754A requires a Safety Program Plan (SPP), which details the processes and related activities that must be conducted. Similarly, RTCA DO-278A requires a Plan of Software Aspects of Approval (PSAA), and RTCA DO-254 requires a Plan for Hardware Aspects of Certification (PHAC). Each developer must describe the compliance plan in the SPP, PSAA, and PHAC, which are provided to the approval authority along with the compliance gap analyses. The SPP, PSAA, and PHAC must be summarized or referenced in the SSPP and the PSP.

Conducting these compliance gap analyses is not a specific safety responsibility. Typically, this effort is led by the PO acquiring the new system or proposing changes to an existing system. This is done with help from the prime contractor conducting systems integration and the subcontractor(s) responsible for developing the software/electronic hardware. Ideally, it should be performed before the contract award as a way to evaluate different vendors, but this is not always technically practical. Other key participants in the process are the PO / approval authority and the development assurance SME (i.e., someone who has qualified skills and knowledge related to software assurance, specifically related to standards and processes, and who is acceptable to the approval authority).

9.6 Managing Software Risk

Analyzing hazards that are introduced by software, or wherein software is one of several contributing factors, is different from analyzing hazards that can be caused by hardware that fails or wears out. Some of the unique characteristics of software include:

- Software follows the Software Development Lifecycle (SDLC), resulting in robust outcomes. Successive steps of the following eventually reach an acceptable failure ratio: (1) architecture, design, coding, and development (changes); (2) Quality Assurance / testing (including logic, flow, load, stress, automation, regression, and union); (3) demonstration (user acceptance); (4) release (with configuration freeze); and

(5) “hot fixes.”[3] Field failures often arise with unplanned, last-minute enhancements and backtracking.

- Software does not wear out. When software fails, it may be due to a design or implementation defect that has always existed (i.e., a latent defect), a recent enhancement that has not undergone the full SDLC, or a change in the operating environment that the software was not designed to accommodate.
- Software usually fails without warning. Robust software includes error detection and correction functions to find and fix typical problems using “restores,” “restarts,” and optimization tools. Abnormal error conditions, unexpected process terminations, and long-duration problems not encountered during testing may still arise. Latent defects, specification errors, and issues with enhancements may have existed before the release of the product and may only be triggered or recognized once many software modules are in broad use under a variety of field operating conditions.
- Software can be more complex than hardware. It is common for device software to consist of hundreds of thousands (or millions) of lines of code. Reuse of existing code modules helps reduce errors. Device software may also be integrated with commercial off-the-shelf system software, such as operating systems that can easily reach similar sizes.
- It is difficult to test all software in a device and nearly impossible to test all combinations of inputs and branching. Modular design helps isolate code into independent blocks.
- A line of software code can be easily changed; however, determining the consequences of that change is more difficult.
- Seemingly insignificant changes in one area of software functionality can lead to defects in unrelated areas of functionality.
- Requirement validation is most effective when analysis is performed early in the development of the requirements.

Software design must be completed at a level of rigor commensurate with the severity of any identified hazard. RTCA DO-278A is the preferred means for implementing this level of rigor. This requirement spans the FAA Acquisition Management System lifecycle and includes In-Service Management. Any changes to fielded software that is already RTCA DO-278A compliant must maintain that compliance. If the original vendor is making the changes, then that vendor must continue to follow their accepted development processes. However, if product development and maintenance have been transferred to FAA Second-Level Engineering, whereby Second-Level Engineering is developing software, then that organization must also follow an RTCA DO-278A–compliant process when making the change.

9.7 Managing Hardware Risk

The following are possible risks in developing system hardware:

- Hardware products consist of physical components that cannot be engineered after manufacturing and cannot add new capabilities that require hardware changes.

3. A “hot fix” is a single, cumulative package that includes information (often in the form of one or more files) that is used to address a problem in a software product (i.e., a software bug). Typically, hot fixes are made to address a specific customer situation.

- Designs for new hardware are often based upon earlier-generation products, but they commonly rely on next-generation components not yet present.
- Hardware designs are constrained by the need to incorporate standard parts.
- Specialized hardware components can have much longer lead times for acquisition than for software.
- Hardware design is driven by architectural decisions. More of the architectural work must be done up front. Thus, it is harder to make unplanned changes.
- The cost of hardware development rises rapidly towards the end of the development cycle. Testing software commonly requires developing thousands of test cases. Hardware testing involves far fewer tests.
- Hardware testing is commonly done by the engineers creating the product.
- Hardware must be designed and tested to work in various environmental conditions and over varying lengths of time.

Electronic hardware design must be completed at a level of rigor commensurate with the severity of any identified hazard. RTCA DO-254 is the preferred means for implementing this level of rigor.

9.8 PO Approval Process

Systems, software, electronic hardware, and safety SMEs within the PO must review the associated lifecycle processes and associated data to confirm that a system change and associated products comply with the approval basis and the level of rigor required by SAE ARP4754A, RTCA DO-278A, and/or RTCA DO-254. The PO should involve the AJI Safety Case Lead (SCL) in this review, as appropriate. The review process assists the PO / approval authority and system developer in determining whether a project meets the approval basis and satisfies this guidance. The review process does this by providing:

- Timely technical interpretation of the approval basis, applicable guidance, approval authority policy, issue papers, and other applicable approval requirements;
- Visibility into the methodologies being used to comply with the requirements and supporting data;
- Objective evidence that the software project adheres to its approved plans and procedures; and
- The opportunity for the approval authority to monitor SME activities.

Each PO must accept the system development assurance deliverables provided by their developers.

9.9 AJI's Role during Solution Implementation

Evidence of the PO reviews listed in Section 2.3.5.1.3.2 must be submitted to the AJI SCL upon request during the Solution Implementation phase to support the final safety approval process.

Appendix A
Preparing and Implementing Program Safety Plans

Preparing and Implementing Program Safety Plans

1 Background

1.1 Description

A Program Safety Plan (PSP) is the government's integrated management plan for conducting system safety for a particular project or program. By executing a PSP, the government ensures compliance with the provisions of the Air Traffic Organization Safety Management System (SMS) Manual, the Safety Risk Management Guidance for System Acquisitions (SRMGSA), and the Federal Aviation Administration (FAA) Acquisition Management System (AMS). Use of a PSP also ensures that an acceptable level of safety consistent with mission requirements is designed into the system.

The Program Office (PO)[1] (using a Program Safety Team (PST), as appropriate) must develop and tailor a PSP that details the specific safety needs and Safety Risk Management (SRM) and system development assurance requirements of the program; the PO must also update the PSP as the program matures and information changes. This PSP forms the basis of the prime contractor's corresponding System Safety Program Plan (SSPP), which is typically required as a contract deliverable. The prime contractor's SSPP, when approved by the government, binds the contractor to a system safety approach that must be consistent with the government's PSP.

The PSP also stands as the PO's agreement with Safety and Technical Training (AJI)—more specifically, Policy and Performance, AJI-3—to conduct SRM and system development assurance in a way that is consistent and compliant with the SMS Manual. The PSP defines the roles and responsibilities of the PO / PST members as they implement system safety. As such, the PSP must describe:

- The SRM and system development assurance efforts that will be applied to each project, sub-system, and interface to support program activities and SMS/SRM requirements;
- The responsibilities of the PO/PST;
- The relationship between the PO and the AJI Safety Case Lead (SCL) throughout the AMS life cycle, but particularly during the Solution Implementation (SI) phase;
    - This includes establishing periodic SCL/PO compliance reviews of the SRM and system development assurance documentation that the PO will develop and approve;
- Planned SRM efforts; and
- A summary of or a reference to the system development assurance program (either as proposed or as documented).

2 System Safety Considerations

System safety must be planned as an integrated and comprehensive safety engineering effort that is sequential and continual. It is essential that the developer's SSPP, as required by the Statement of Work in the developer's contract, aligns and is consistent with the government's

1. As a program moves through the AMS lifecycle (i.e., from Concept and Requirements Definition to the Investment Analysis phase, through the Solution Implementation phase, and ultimately into In-Service Management), program management responsibilities transfer from the Assistant Administrator of the Office of NextGen to Mission Support Services, the PO, or Technical Operations.

PSP. In addition, the timing of the required safety analyses must be consistent with the engineering milestones outlined in the FAA Systems Engineering Manual (SEM). A Data Item Description (DID) detailing the SSPP requirements must be placed on contract. The specific delivery timeframes and review processes for a DID must be included in the Contract Data Requirements List.

In addition:

- Any SRM panel facilitated or conducted by the developer (i.e., to develop a Sub-System Hazard Analysis or a System Hazard Analysis) must include Subject Matter Experts (SMEs), particularly those with an operational perspective. This must be reflected in both the PSP and the SSPP and within the developer's contract.
- The government must actively review and be able to modify/comment upon the safety analysis documentation as it is being prepared by the developer (i.e., not just at its final delivery). This must be reflected in both the PSP and the SSPP and within the developer's contract.
- An approved PSP must be in place prior to any Joint Resources Council (JRC) milestone decision or In-Service Decision (ISD) per AMS policy. As system functionality is often operationally released in segments or phases, there may be multiple ISDs for an acquisition or modification to an existing National Airspace System (NAS) system. The PSP to support the Final Investment Decision (FID) must discuss the Initial Operating Capacity (IOC) / ISD strategy (i.e., required number of IOCs/ISDs) documented in the Implementation Strategy and Planning Document (ISPD). It is possible that separate PSPs may be required for each segment/phase.
- If the deployment strategy is not well defined at the FID, the ISD strategy may simply state that the entrance criteria for an ISD (i.e., test, security, safety, and Independent Operational Assessment (IOA)) will be met for each release/phase of the deployment. In this situation, the PSP may need to be updated during the SI phase to accurately reflect the final ISD strategy. In addition, if the deployment strategy changes, the JRC requires that the ISPD be updated to incorporate the changes; the PSP may also need to be updated if these changes affect the IOC/ISD and/or safety strategy.
- The PSP must reference the version (i.e., the publication date) of the SRMGSA / SMS Manual in effect when the PSP was prepared. However, the PSP must be updated at each JRC decision point. The versions of the SRMGSA / SMS Manual at the FID will become the operative documents that the PO must follow for the remainder of the program unless the program is restructured via a change in scope, segmentation, or rebaselining. The PO must consult with the AJI SCL for advice when this has occurred because the approved PSP may no longer apply, and the PSP may need to be updated.
- The PSP must summarize or reference the system development assurance plans as proposed or when they are finalized.
- If the PO is planning on using alternate methods for conducting SRM / system development assurance (see Section 7), this must be discussed at the Safety Strategy Meeting (SSM) with the AJI SCL. If he/she approves the use of the alternate method(s), this decision must be documented in an approved PSP.
- Prior to developing the PSP, the PO must contact the AJI SCL to conduct an SSM to discuss the tailoring of any safety documentation and other SRM considerations (see Section 5.1). For a Technology Refreshment (TR) portfolio, it is possible that the

complexity of projects within the portfolio may warrant the development of project-specific PSPs to supplement the portfolio PSP; this need must be detailed in the approved portfolio PSP. There is no need to develop project-specific PSPs for sub–Acquisition Category 2 TR projects; however, the approved portfolio PSP must outline the SRM and development assurance requirements for these projects.

3 Preparing the PSP

This section summarizes the key steps in preparing a PSP:

1. Identify system safety requirements
2. Develop a safety strategy based on these requirements
3. Translate the developed system safety strategy into a PSP
4. Submit the PSP for approval and signature

3.1 Identify System Safety Requirements

The PO must identify system safety requirements as an initial step necessary to developing/tailoring a program's safety strategy. The PO, the PST, the AJI SCL, the Office of NextGen, and other stakeholders must collaborate to identify the requirements and solidify them via one or more SSMs. The AJI SCL may also recommend language to be included in any contracts to enhance the government-developer system safety interface. The identification process consists of several sub-steps, as documented below.

3.1.1 Review Generic System Safety / SMS and AMS Program Requirements

The PO / PST must review generic source documentation such as the AMS (specifically, AMS, Section 4.12, *National Airspace System Safety Management System*), the SMS Manual, the SRMGSA, and applicable FAA orders (e.g., FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*, and FAA Order 8040.4, *Safety Risk Management Policy*). This must be done to determine the prescribed safety requirements the program must meet at each acquisition milestone.

3.1.2 Identify Mechanism for Tracking and Monitoring Program Hazards

FAA Order JO 1000.37 requires that all identified safety hazards and their safety risks be recorded in a database. The PO/PST must use the Safety Management Tracking System (SMTS) to enter data from safety analyses/assessments (including all low-, medium-, and high-risk hazards) before beginning the monitoring process. In the PSP, the PO/PST must include plans for using SMTS and for ensuring that personnel have been trained to use this system. (Refer to Section 8.5 of the SRMGSA for further information regarding SMTS.)

3.1.3 Identify Development Assurance Requirements

The PO must evaluate how new and/or modified systems will comply with system development assurance practices and standards.

The PSP must include a discussion of these processes (or acceptable alternatives):

- System development assurance per SAE Aerospace Recommended Practice (ARP)[2] ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*;

2. An ARP is a guideline from SAE International.

- Hardware development assurance per RTCA[3] DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*; and
- Software development assurance per RTCA DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*.

The PSP must discuss contractual requirements and describe how the PO intends to prove that the developer is complying with the requirements. The PSP must provide details about the planned activities (including checklists that will be used) and timelines/milestones for submittals, reviews, and audits.

The PSP must address the following topics for system development assurance compliance:

- The activities the vendor's Quality Assurance (QA) team will conduct on the development to ensure compliance;
- The activities the PO will conduct about the vendor's QA oversight activities;
- The activities the PO will conduct about the vendor's development to validate compliance;
- The PO's process for approving vendor-submitted documents; and
- The nature of the PO's working relationship with the AJI SCL during the SI phase of the program.

Techniques described in the FAA SEM may be used in performing these tasks. For example, the N^2 analysis is a recommended way to evaluate the vendor's development processes because it highlights inputs and outputs for each process and relationships to other processes. These techniques can be used to determine whether each process is adequately defined and has transition criteria for entering the next process.

3.1.4 Identify IOC Safety Requirements

First-site IOC occurs when the operational capability is declared ready for conditional or limited use by site personnel (i.e., after the capability is successfully installed and reviewed at the site, and site acceptance testing and field familiarization are completed). The IOC requires that operational requirements are satisfied and that full logistics support and training are in place for technicians and air traffic specialists. The PSP must include the specific safety requirements that must be satisfied before the IOC can be declared.

3.1.5 Identify Post-Implementation Review Safety Requirements

A Post-Implementation Review (PIR) is an evaluation tool used to assess results of designated investment programs against baseline expectations 6 to 24 months after they go into operational service. Its main objective is to determine whether a program is achieving expected performance targets (including those resulting from safety requirements) and meeting the service needs of the customers. The PIR seeks to validate the original program Business Case. The PIR also seeks to provide lessons learned with regard to the original program Business Case for application on future Business Cases. A PIR strategy is developed in the AMS

3. RTCA, Inc., is a private, not-for-profit association founded in 1935 as the Radio Technical Commission for Aeronautics; it is now referred to simply as "RTCA."

lifecycle during the Final Investment Analysis and must include appropriate safety considerations, which the PO must incorporate into the PSP.

3.1.6 Develop a Nominal Safety Program Schedule

Because there must be an approved PSP in place at each major decision point after the Concepts and Requirements Definition phase (i.e., the Investment Analysis Readiness Decision (IARD), Initial Investment Decision (IID), FID, and ISD), the PO / PST must develop a nominal safety program schedule consistent with JRC decision points. In addition to JRC decision points, key AMS milestones after the FID—including plans to verify the incorporation of design safety requirements through inspection (e.g., design reviews/audits), testing (e.g., developmental testing and evaluation), or performance assessment (e.g., IOA or other operational testing and evaluation)—must be aligned with the contract schedule. The schedule must also include a requirement for a safety review prior to the IOC being declared.

3.2 Develop a Safety Strategy based on Identified Program Requirements

Given the identified program safety requirements (and any sub-requirements at the testable level of design or performance), the PO must develop a safety strategy that is tailored to meet the program's needs. This strategy preparation is done at SSMs with the help of the AJI SCL (who may consult with AJI-3 management as necessary, particularly if a large amount of document tailoring is under consideration).

3.2.1 Prepare a Safety Strategy Worksheet

To prepare for the SSMs, the PO/PST must first prepare a Safety Strategy Worksheet (SSW), which is supplied by the AJI SCL. At a minimum, the SSW must contain the following information:

- System/Program name and previous program name, if any;
- Short system description;
- System/FAA/External interface(s);
- Interdependencies;
- Changes to legacy systems, if any;
- Name and phone number of key individuals: PO, PST Lead, AJI SCL, applicable Service Unit SMEs, and development assurance SMEs;
- Where the program is in the AMS lifecycle;
- Any plan for combining JRC decision points;
- Whether alternative solutions may be proposed;
- Proposed dates of the JRC investment decisions and the IOC/ISD;
- Impact of the system on the NAS, separation, navigation, communications, and aircraft;
- A list of any safety analyses/assessments completed to date and a summary of any safety findings, including potential safety risk impacts of the system on the NAS;
- Traceability to a Next Generation Air Transportation System (NextGen) portfolio, including any requirements allocated from the portfolio;

- Traceability to NAS Enterprise Architecture (EA) elements (e.g., systems, functions, operational activities, information exchanges, and data exchanges) (this may be provided in the form of previously delivered program-level NAS EA products);
- Traceability to any previously conducted AJI SCL–authorized analyses and assessments that impact the program; and
- IOA designation, if applicable.

3.2.2 Organize and Hold the First SSM

The purpose of the SSM is to review the SSW to ensure the PO, the AJI SCL, and other stakeholders:

- Have a common understanding of the program's safety requirements;
- Outline the acquisition's required SRM documents;
- Set a schedule for document preparation, the peer review process, coordination with other lines of business as needed, and approval;
- Tailor and streamline the full acquisition process for proposed actions of less-than-full acquisition or non-acquisition solutions; and
- Determine and obtain copies of any prior SRM documents, safety analyses, or safety assessments that may have value in this proposed action (i.e., concept SRM documents turned into investments; portfolio SRM documents broken out into single systems; or legacy SRM documents for replacement, reconfiguration, policy change, or other hard-to-classify, non-acquisition actions).

The outcome of the SSM is a safety strategy that is mutually agreed upon by the PO, AJI SCL, and other stakeholders. Additional SSMs may be held as the program matures; the safety strategy may be revised and made more discrete, resulting in a need for the PSP to be updated.

3.3 Translate the Developed System Safety Strategy into the PSP

The PSP supports the entire range of activities in every phase of the program. The PO must develop the agreed-upon safety strategy into a plan that includes the following information (at a minimum):

- Program scope and objectives;
- Description of the range of alternatives, alternative systems, and generic capability (at the IARD);
- Program safety organization/management information;
- Program stakeholders;
- Safety program milestones;
- General safety requirements and criteria, including their traceability to NextGen portfolios;
- Impact of the system on the NAS (including separation assurance, navigation, communications, and aircraft safety, as applicable);
- Hazard analyses to be performed;

- Processes for using SMTS;
- Potential safety performance metrics, including safety performance indicators, initial baseline values, and residual target values;
- Safety requirements management;[4]
- Safety assessment review plan (i.e., the type of safety assessment program to be used and scheduled for accomplishing safety verification and validation);
- Safety management of program changes (e.g., scope, design, and schedule);
- Safety training required;
- Development assurance considerations (e.g., applicability, development assurance level considerations, and architectural mitigation);
- Safety interfaces with development engineering, support contractors (pre-FID), prime contractors (post-FID), management, and other specialty engineering groups;
- The relationship between the PO and the AJI-314 SCL, including a description of their planned interaction during the SI phase of the AMS;
- Dependencies on other PSPs; and
- IOA designation with justification, if applicable.

3.4 Submit the PSP for Approval and Signature

The following steps are required to obtain approval for each iteration of the PSP:

- The PST Lead (as designated by the PO) prepares, signs, and submits the PSP to the PO for approval.
- The PO either signs the PSP or returns the document to the PST Lead for further coordination, as necessary. Upon PO approval, the Director of the PO in which the system is located must also approve the PSP before it is sent to AJI.
- The PSP is submitted to the AJI SCL for coordination (e.g., peer review), approval, and final signature by AJI-3.

Upon approval, the PO must upload the PSP to SMTS.

4 Implementing the PSP

4.1 Coordinate with the Contractor

Once the PSP is approved, the PO must implement the PSP as agreed upon with the support of the PST. The PO must also coordinate with the prime contractor to ensure that SSPP-defined safety efforts are being implemented and that they support the safety tasks in accordance with the PSP.

4.2 Monitor the Progress of PSP Implementation

The PO must ensure the PSP is implemented per the agreed-upon schedule (which is subject to revision under certain circumstances) and inform the AJI SCL of any deviations from the plan.

4. The purpose of safety requirements management is to ensure that the FAA documents, verifies, and meets the needs of its internal and external stakeholders. Verification and validation of safety requirements must be conducted to ensure the traceability of safety requirements to both the hazards and NAS capabilities.

The PO must also ensure that safety analysis/assessment results are entered into SMTS to enhance AJI's ability to monitor the safety program. The AJI SCL must also monitor the safety program and the system development assurance program on a regular basis, particularly as JRC milestones approach and as certain required documentation must be approved.

4.3 Update the PSP

The PSP is a living document that the PO must update as circumstances change (e.g., during different acquisition phases or when changes are made to the program structure/management team, program financial profile, and/or program approach). Therefore, the PO must review the PSP periodically and update it to ensure all the requirements identified in the SRMGSA are accounted for and sufficient details exist in the plan for execution. Each PSP update must be approved by AJI-3.

The initial PSP, at either the IARD or the IID, may be based only on the high-level safety objectives developed in the Operational Safety Assessment. At this stage, the PSP should at least acknowledge that, depending on the architectural implementation of the operational solution, there may be further allocation of safety requirements to the system as it matures (i.e., development assurance standards may come into play). The PSP at the FID must reflect the safety requirements that are in the final Program Requirements Document along with the required verification means.

The PSP must be reviewed prior to each AMS investment decision and before the IOC or ISD is declared. If agreements made in the original PSP need to be amended, then the PO must resubmit the revised PSP to AJI-3 for approval.

Appendix B
Overview of the System Safety Program Plan

Overview of the System Safety Program Plan

1 Background

1.1 Description

A System Safety Program Plan (SSPP), if contractually required and when approved, becomes a binding agreement between the Federal Aviation Administration (FAA) and the contractor regarding how the contractor will meet contractual requirements for system safety.

The SSPP describes in detail the contractor's safety organization, schedule, procedures, and plans for fulfilling contractual system safety obligations. The SSPP becomes the management vehicle for both the FAA and the contractor to ensure that proper management attention, sufficient technical assets, correct analysis and hazard control methodology, and tasks are planned in a correct and timely manner. Once approved, the FAA uses the SSPP to track the progress of the contractor's System Safety Program (SSP).

The SSPP is valuable to the contractor as a planning and management tool that establishes a "before-the-fact" agreement with the FAA on how the SSP will be executed and to what depth. The approved SSPP serves as the SSP baseline that will minimize the potential for downstream disagreement of SSP methodology.

1.2 Purpose of the SSPP

The SSPP accomplishes the following:

- Contains the scope, contractor organization, program milestones, safety requirements, safety data, safety verification, accident reporting, and safety program interfaces;
- Describes the contractor's plan for implementing safety requirements;
- Identifies the hazard analysis and safety risk assessment processes that the contractor will use;
- Defines how the contractor will record hazards and predicted residual risk levels and how they will be formally accepted and tracked;
- Provides the FAA an opportunity to review the contractor's scheduling of safety tasks in a timely fashion, permitting corrective action when applicable; and
- Describes how the contractor will comply with system development assurance processes per SAE Aerospace Recommended Practice (ARP)[1] ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*; RTCA[2] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*; and RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*, or equivalent processes and their supporting supplements. (The SSPP should act as the contractor's compliance plan for development before their Safety Program Plan, Plan for Software Aspects of Approval, and Plan for Hardware Aspects of Certification or equivalent plans are developed.) The SSPP should also include the contractor's anticipated delivery date for these plans and

1. An ARP is a guideline from SAE International.

2. RTCA, Inc., is a private, not-for-profit association founded in 1935 as the Radio Technical Commission for Aeronautics; it is now referred to simply as "RTCA."

an initial estimate of how many Configuration Indexes are anticipated to accompany the different system releases.)

- Ideally, these plans should be approved prior to the beginning of any design work.

2 Developing the SSPP

2.1 Establishing the Contractual Requirement

The FAA Contracting Office, with Program Office (PO) input, must establish the contractual requirements for an SSPP in the Statement of Work (SOW). An appropriate Data Item Description (DID) for an SSPP which outlines its required contents must be included as part of the contract.

The FAA usually requires that the contractor submit the SSPP as a deliverable for approval 30 to 45 days after the start of the contract. In some situations, the FAA may require that a preliminary SSPP be submitted with the proposal to ensure that the contractor has planned and budgeted for an adequate SSP. Since the system safety effort can be the victim of a cost competitive procurement, an approval requirement for the SSPP provides the FAA the necessary control to minimize this possibility.

2.2 Elements of an Effective SSPP

An effective SSPP clearly details these four elements:

- A planned approach for task accomplishment
- Availability of a qualified staff to accomplish tasks
- Authority to implement tasks through all levels of management
- Appropriate staffing and funding resources to ensure completion of tasks

An effective SSPP must demonstrate safety risk control planning through an integrated program management and engineering effort and be directed toward achieving the specified safety requirements of the SOW and system specification. The plan must include details about the methods the contractor will use to implement and comply with each system safety task described by the SOW and the safety-related documentation listed in the contract. The SSPP must list all requirements and activities required to satisfy the SSP objectives, including all appropriate related tasks. A complete breakdown of system safety tasks, subtasks, and resource allocations for each program element through the term of the contract must also be included.

The SSPP must not be generic. Rather, the contractor must tailor the system safety approach to be specific to the contracted program at the contractor's facilities. The SSPP must describe the system safety aspects and interfaces of all appropriate program activities. This includes integrating into the SSP any system safety activities (such as hazard analyses) conducted by any subcontractors.

The plan must describe an organization featuring a system safety manager who is directly responsible to the contractor’s Program Manager or his or her agent for system safety. This agent must not be organizationally inhibited from assigning action to any level of program management. The plan must further describe methods by which critical safety problems are brought to the attention of program management and for management approval of closeout action.

There must be a close relationship and consistency between the PO's approved Program Safety Plan (PSP) and the contractor's SSPP. Whereas the PSP represents the PO's agreement with Safety and Technical Training with regard to how the SSP should be conducted, the SSPP is the PO's similar agreement with the contractor.

2.3 SSPP Contents

The SSPP must detail:

- The contractor's program scope,
- Safety organization,
- Program milestones,
- Requirements and criteria,[3]
- Hazard analyses,
- Safety data,
- System development assurance activities,
- Verification of safety requirements,
- An auditing and monitoring program,
- Training,
- Accident and incident reporting, and
- Interfaces.

2.3.1 Contractor's Program Scope

The SSPP must include a systematic, detailed description of the scope and magnitude of the overall SSP and its tasks. This includes a breakdown of the project by organizational component, safety tasks, subtasks, events, and responsibilities of each organizational element, including resource allocations and the contractor's estimate of the level of effort necessary to accomplish the contractual task effectively. The SSPP must also define a program that satisfies the system safety requirements imposed by the contract.

2.3.2 Safety Organization

The SSPP must describe:

- The system safety organization or function as it relates to the program organization, including a description of the lines of communication and the position of the safety organization within the program;
- The responsibility and authority of all personnel with significant safety interfaces;
- The staffing plan of the system safety organization for the duration of the contract;
- The procedures by which the contractor will integrate and coordinate the system safety efforts; and
- The process by which contractor management decisions will be made.

3. Criteria are principles or standards against which actions may be judged. The government needs this information because it may not know all the internal/external standards that a contractor will follow as part of its SSP.

In addition, the SSPP should note that the system safety manager must be responsible for:

- Internal control for the proper implementation of system safety requirements and criteria affecting hardware, operational resources, and personnel by interfacing with other program disciplines, and
- The initiation of required action whenever internal coordination of controls fails in the resolution of problems.

2.3.3 Program Milestones

To be effective, the system safety activities for any program must be integrated into other program activities. For the sake of efficiency, each SSP task must be carefully scheduled to have the most positive effect. A safety analysis performed early in the design process can lead to the inexpensive elimination of a hazard through design changes. The later the hazard is identified in the design cycle, the more expensive and difficult the change to address it. Hazards identified during production or following deployment may be impractical to change. In such cases, hazards may still be controlled through procedural and training steps; however, doing so when the hazards could have been prevented reflects unnecessary, long-term costs and risk.

The SSPP must provide the timing and interrelationships of system safety tasks relative to other program tasks. The schedule for each SSP task in the SSPP should be tied to a major milestone (e.g., start 30 days before the preliminary design review) rather than a specific date. This approach ensures that the SSPP does not need revision whenever the master program schedule shifts. The same programmatic control is maintained through the program master schedule without the associated cost of documented revision or schedule date waiver.

2.3.4 Requirements and Criteria

A formally submitted SSPP provides the opportunity for the PO and the contractor to reach the same understanding of technical and procedural requirements and plans before precious assets are expended. The inclusion of this information expedites reaching a common understanding between the PO and the contractor. This information includes:

- Safety performance requirements,
- Safety design requirements, and
- Documentation.

2.3.5 Hazard Analyses

The SSPP must describe the specific analyses to be performed during the SSP and the methods to be used to perform these required analyses.

2.3.6 Safety Data

The SSPP must show the basic data flow path to be used by the contractor. This information must show where the system safety activity includes reviewing internally generated data and the requirement for a contractor to maintain a system safety data file.

2.3.7 System Development Assurance Activities

The SSPP must include the system, software, and electronic hardware development assurance activities per SAE ARP4754A, RTCA DO-278A, and RTCA DO-254 or alternate processes, including the allocation of the identified Functional Development Assurance Levels (DALs) into

the sub-system and how these will be assigned as Item DALs of the software and electronic hardware configuration items.

2.3.8 Verification of Safety Requirements

Safety verification must be demonstrated by implementing a dedicated safety verification test and/or assessment program. The SSPP must include:

- The verification (e.g., test, analysis, and inspection) requirements for ensuring that safety is adequately demonstrated and the verification results are documented,
- Procedures for confirming test information is transmitted to the FAA for review and analysis,
- Procedures for ensuring the safe conduct of all tests, and
- Reviews and audits evaluating development assurance safety requirements.

2.3.9 Auditing and Monitoring Program

The contractor's SSPP must describe the techniques and procedures to be used in ensuring the accomplishment of internal and subcontractor SSPs. The prime contractor must conduct audits of major vendors, when appropriate. The contractor must ensure that hazard traceability is maintained.

2.3.10 Training

The SSPP must contain the contractor's plan for using the results of the SSP in various training areas. As the SSP will produce results that should be applied in training operator, maintenance, and test personnel, procedures must account for transmitting hazards that relate to any activity preparing training plans. Training must not only be continuous—it must also be conducted both formally and informally as the program progresses. The SSPP must also address training devices.

2.3.11 Accident and Incident Reporting

The contractor must notify the PO immediately in case of an accident. The SSPP must include the details and timing of the notification process. The SSPP must also define the time and circumstances under which the PO assumes primary responsibility for accident and incident investigation. The support provided by the contractor to FAA investigators must be addressed. The procedures by which the PO will be notified of the results of contractor accident investigations must be detailed. Provisions must be made for an FAA observer to be present for contractor investigations. Any incident that could have affected the system must be evaluated from a system safety point of view. In this case, an incident is any unplanned occurrence that could have resulted in an accident. Incidents involve the actions associated with hazards, both unsafe acts and unsafe conditions that could have resulted in harm.

2.3.12 Interfaces

Since conducting an SSP will eventually affect almost every other element of a system development program, a concerted effort must be made to effectively integrate support activities. Each engineering and management discipline often pursues its own objectives independently, or at best, in coordination only with mainstream program activities such as design engineering and testing. To ensure that the SSP is comprehensive, the contractor must impose requirements on subcontractors and suppliers that are consistent with and contribute to the overall SSP. The SSPP must show the contractor's procedures for accomplishing this task.

The prime contractor must evaluate variations and specify clear requirements tailored to the needs of the SSP.

Occasionally, the PO procures sub-systems or components under separate contracts to be integrated into the overall system. Subcontracted sub-systems that affect safety must be required to implement an SSP. If specified in the contract, the integration of these programs into the overall SSP is the responsibility of the prime contractor for the overall system. The prime contractor's SSPP must indicate how the prime contractor plans to affect this integration and what procedures will be followed in the event of a conflict.

3 Approving the SSPP

The SSPP is a contract deliverable that must be approved by the PO in accordance with the contract and Program Management Organization procedures.

Appendix C
Conducting and Documenting an Operational Safety Assessment

Conducting and Documenting an Operational Safety Assessment

1 Background

1.1 Description

Unless specifically waived by an approved Program Safety Plan (PSP), the Program Office (PO)[1] must conduct an Operational Safety Assessment (OSA) to identify, analyze, and document operational hazards and associated safety objectives and requirements early in the Federal Aviation Administration (FAA) Acquisition Management System (AMS) planning phase. The OSA is an indispensable tool for allocating safety objectives and requirements to lower-level increments. This early identification will improve safety and product integration, enhance product performance, and increase the probability of program success.

An OSA may be prepared to provide the system designers and management with a set of safety goals for design. In this phase, the results of any early safety analyses/assessments that affect the program (e.g., a Functional Hazard Assessment (FHA)) are inputs to the OSA. (See Appendix D.) Certain planning must occur prior to the Investment Analysis Readiness Decision (IARD), such as the development of the Business Case Analysis Report and the preliminary Program Requirements Document (pPRD), which may require input from the OSA.

Unlike follow-on safety analyses/assessments, an OSA does not consider overall safety risk; rather, the PO must use the OSA to (1) assess hazard severity and (2) determine the target level of likelihood required to achieve an acceptable level of safety and Development Assurance Levels (DALs). In other words, OSA-identified severity levels must be mapped to preset levels of likelihood and DALs, establishing the necessary safety levels required for controlling a hazard. This means that a hazard with a catastrophic severity level would be mapped to a likelihood level and DAL requirement that are more stringent than that of a hazard with a minor severity level. This process establishes the level needed for controlling the hazard at or below a medium risk level, and it assists in establishing safety requirements for the concept or system design.

The PO must use a Safety Risk Management (SRM) panel to conduct the OSA. The PO must identify approval authorities and stakeholders needed to establish and demonstrate compliance with requirements for the air traffic service provision, its use, and any related Communication, Navigation, and Surveillance (CNS) / Air Traffic Management (ATM) system. Some stakeholders may also be SRM panel members, in accordance with the Air Traffic Organization (ATO) Safety Management System (SMS) Manual.

The PO must conduct an OSA in preparation for the IARD phase of the AMS lifecycle.

1. As a program moves through the Federal Aviation Administration Acquisition Management System lifecycle (i.e., from Concept and Requirements Definition to the Investment Analysis phase, through the Solution Implementation phase, and ultimately into In-Service Management), program management responsibilities transfer from the Office of NextGen to Mission Support Services, the PO, or Technical Operations.

1.2 Overview

Figure C.1 provides a high-level overview of the basic OSA methodology.

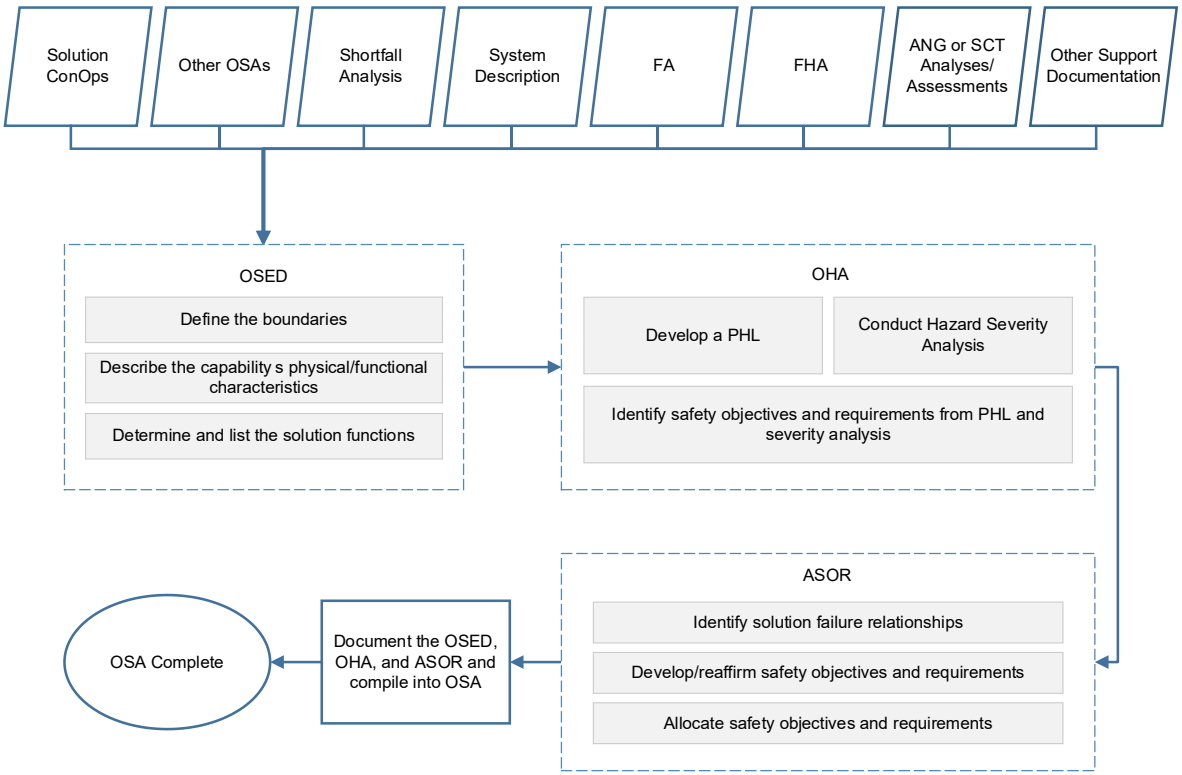

Figure C.1: OSA Inputs, Components, and Methodology

2 OSA Inputs

2.1 System Description

The system description provides information that serves as the basis for identifying all hazards and associated safety risks. The system must be described and modeled in sufficient detail to allow the safety analysis to proceed to the hazard identification stage.

2.2 FHA

An FHA is not a required AMS safety assessment, but if one is conducted, it can be a useful input for the OSA (particularly when complex systems are being developed).

2.3 Solution Concept of Operations

The Solution Concept of Operations (ConOps) paints a picture of the ideal solution to an identified need or shortfall. It describes how users will employ the new capability within the operational environment and how it satisfies the service need. This document includes descriptions of the characteristics of the proposed solution, the environment in which the solution will operate, and the responsibilities of the users.

2.4 Office of NextGen– or Safety Collaboration Team–Mandated Safety Analysis/ Assessment Reports

Safety analysis or assessment reports mandated by the Office of NextGen (ANG) or the Safety Collaboration Team (SCT) provide high-level information that may be relevant to the OSA. This

information may include proposed safety requirements and candidate hazards specifically targeted to the increment that the OSA addresses.

2.5 Operational Services and Environment Description

Although the Operational Services and Environment Description (OSED) is described herein as an element of the overall OSA, an OSED may have already been developed as part of a Solution ConOps or an SCT-mandated analysis/assessment. If so, that OSED may be used as input or further developed for the OSA.

2.6 Functional Analysis

A Functional Analysis (FA) examines a solution's functions and sub-functions that accomplish the operation or mission. An FA describes what the solution does, rather than how it does it, and is conducted at a level needed to support later synthesis efforts. Products from the FA, such as the Functional Flow Block Diagram (FFBD) and N^2 diagram, may be used as inputs when developing the OSA. Other techniques may also be used to diagram solution functions.

The outcome of the FA process is a functional architecture. Since the functional architecture may be further refined during the Investment Analysis phase of the AMS lifecycle, a stable FA, even at a high level, may be unavailable before the IARD in sufficient time to be a meaningful, enabling input to the OSA. Therefore, the OSA should address the solution using a preliminary or an initial functional architecture; however, changes should be anticipated as the FA is developed in parallel with the OSA prior to the IARD.

2.7 Other OSAs

OSAs developed for other solutions/capabilities may be important inputs to an OSA.

2.8 Shortfall Analysis

A Shortfall Analysis describes the difference or shortfall between the current service and the desired service. The Shortfall Analysis Report is refined and updated before the IARD. It quantifies the problem as well as its nature, urgency, and impact in operational terms (e.g., airborne or ground delays and accident rate) and describes the potential benefits of the initiative and the in-service improvements that could be expected. The Shortfall Analysis Report may provide information useful for identifying potential hazards in an OSA.

2.9 Other Support Documentation

Documentation relating to existing design, tests, field performance, National Airspace System (NAS) operations research, and detailed support (e.g., recent SRM documents or portfolio SRM documents) may already exist for the replacement, removal, or reconfiguration of existing NAS systems; these documents may apply substantially to the new proposed action. The PO should consider conducting an audit for applicable and reusable baseline documents and SRM documents that can form a sound basis for legacy architecture, requirements, design, performance, and known NAS constraints.

3 OSA Components

3.1 OSED

The OSED describes the service characteristics of the solution concept in an operational environment. This description includes both ground and air elements and must include all elements of the 5M Model (as discussed in the current version of the SMS Manual). The OSED is used as a mechanism to describe the services provided by the solution, the users of the solution, and the varying operational and environmental considerations in which the service is

provided for the related CNS/ATM system. The description provided by the OSED is used as a baseline and solution boundary from which to conduct the safety assessment. The OSED captures elements that comprise a CNS/ATM system (e.g., aircraft equipage, air traffic service provider technical systems, communication service provider systems, and procedural requirements), and it includes the operational performance expectations, functions, and selected technologies of the CNS/ATM system.

3.1.1 OSED Development Process

The OSED facilitates the formulation of technical and procedural requirements based on operational expectations and needs. The OSED development process is described below.

3.1.1.1 Define the Boundaries

Define the boundaries of the solution under consideration, including anticipated interfaces, a technology's independent layers, and common services among NAS systems and sub-systems (both internal and external). Determine, separate, and document which elements of the solution to describe and analyze for hazard identification. Identify shared resources (if any) for which independent SRM was already performed.

3.1.1.2 Describe the Physical and Functional Characteristics of the Solution's Concept

Using models such as those described in the SMS Manual (e.g., the 5M Model), describe:

- The concept's state by including physical and functional characteristics,
- The environment's physical and functional characteristics,
- Air traffic services to be provided,
- Affected human elements (e.g., pilots, controllers, maintenance personnel, and supervisors), and
- Operational procedures related to or affected by the concept.

3.1.1.3 Determine and List Functions

Using the concept description and preliminary input from the FA or other sources, identify and list the required functions (including those that are performed by the users). For example, the primary function of a precision navigation system is to provide Air Traffic Control (ATC) and flight crews with vertical and horizontal directional guidance to the desired landing area. If desired, these functions could be split into vertical and horizontal guidance. Supporting functions would be those that provide the solution with the ability to perform the primary function. A supporting function of the precision navigation system would be the transmission of the radio frequency energy for horizontal guidance. The PO must determine how to group these functions and to what level of rigor the analysis should be performed.

3.1.1.4 Develop and Document the OSED

Develop and document the OSED from the information obtained.

3.2 Operational Hazard Assessment

The Operational Hazard Assessment (OHA) assesses the operational hazards associated with the solution/services described in the OSED. It determines the severity of each hazard so that operational objectives and safety requirements can be identified for any solution that results in an acceptable level of safety risk. Once the solution has been bounded and described and the functions have been identified in the OSED, an SRM panel must identify the associated hazards

via an OHA.[2] In developing an OHA, the panel may develop a Preliminary Hazard List (PHL)[3] using a systematic analysis of solution functions and functional failures to identify hazards. Each hazard must be subsequently classified according to its potential severity after considering causes and effects. The OHA uses the severity identified for each hazard to identify safety objectives and safety requirements for the solution that will result in an acceptable level of safety risk.

In general, as severity increases, the safety objectives and safety requirements must be designed to achieve the lowest possible likelihood of occurrence that would result in an acceptable level of safety. A safety objective or "goal" in the context of the OHA is the desire to reduce the likelihood of unacceptable safety risk. The associated safety requirement (i.e., minimum level of acceptable performance) is the means of attaining that objective. The OHA must establish safety objectives that ensure an inverse relationship between the probability of a hazard leading to an incident or accident and the severity of the hazard's outcome. The safety objective should result in the lowest practicable acceptable level of safety risk.

The OHA may be performed using either qualitative or quantitative methods. However, it is preferable to use quantitative data to support the assessment.[4]

3.2.1 OHA Development Process

The OHA[5] development process is described below.

3.2.1.1 Develop the PHL

Develop a PHL, based on the operational hazards identified, that is concise, clear, and understandable; this PHL serves as the repository of the SRM panel's initial efforts to identify all possible hazards. The PHL is refined and matured over time as the SRM panel validates the identified hazards as credible and as the OHA is further developed. A Bow-Tie Model[6] may be used as a tool for distinguishing between hazards, causes, and effects within the PHL.

3.2.1.2 Conduct Analysis to Identify the Operational Hazards

Based on (1) the services/functions provided by the solution that were documented in the OSED and (2) modifying the PHL, identify the operational hazards. Document the analyses undertaken, linking the proposed change to the operational safety of the NAS—specifically the detailed, logical, and analytical connections. For these types of analyses, the most effective method is to focus on the "malfunction of" or the "loss of" each of the identified functions and their outputs. This is best done by "failing" the functions from the developed N^2 diagram or the FFBD, if available.

3.2.1.3 Identify Controls

Identify the controls; the rationale for their inclusion; and any supporting data that confirm the controls' inclusion, applicability, and feasibility related to the hazard under consideration.

2. The SMS Manual provides policy on how to assemble SRM panels and facilitate the SRM process.

3. The concept of the PHL is explained in the SMS Manual.

4. Various databases have been developed to support the SMS. Some of these are listed in the SMS Manual.

5. Refer to the SMS Manual for descriptions of some of the concepts in this section, including a list of analysis tools, the safety order of precedence when identifying controls that mitigate the risk of a hazard, the determination of a hazard's severity, and the identification of safety requirements.

6. The Bow-Tie Model is a diagram of the hazard, its causes, its effects, and the controls that minimize the risk. This methodology is an excellent way of visualizing risk management and communicating the context of the controls (barriers and mitigations) that manage or could manage risk.

Controls are measures, design features, warnings, and procedures that are already in place and mitigate credible outcomes (i.e., they have already been validated and verified as being effective). They may include procedural requirements as well as aircraft or ground system requirements related to the solution under review. The Bow-Tie Model (specifically, the event tree side) can be used to identify controls and safety requirements.

3.2.1.4 Identify Operational Hazard Effects

Determine the effects of each operational hazard by evaluating the services in the solution state (including legacy system considerations) for the intended operational capabilities, as defined in the OSED. The Bow-Tie Model (specifically, the outcome side) can be used for identifying effects.

3.2.1.5 Classify Operational Hazards

Classify each operational hazard according to the severity of its identified effects using the current version of the SMS Manual. When determining severity, the SRM panel must assess all effects of the hazard on operations—taking into account the aircrew, aircraft, and air traffic services—and must use the measure yielding a higher severity (i.e., the most conservative estimate). This enables safety objectives and safety requirements to be given a consistent and objective meaning.

The severity of each hazard is determined by the worst credible outcome or effect of the hazard on the solution or the NAS.

3.2.1.6 Identify Safety Objectives and Requirements

Establish overall safety objectives (either qualitative or quantitative) based on the operational hazard classifications. This includes using SAE Aerospace Recommended Practice (ARP)[7] ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*, or alternate guidance to assign a DAL to each system function based on the severity of its effects on the aircraft. (As the design matures, the DALs may be reduced using architecture.) Once the safety objective is determined for each hazard, safety requirements can be written to ensure that the appropriate hazard controls are established as product requirements. Note that a requirement is a description of what must be done to achieve a safety objective. Safety objectives and controls are independent of each other and should not be duplicated.

3.2.1.7 Document the OHA

Populate an OHA Worksheet with information for all identified hazards and their associated safety objectives and safety requirements. The worksheet categories are described in Table C.1.

7. An ARP is a guideline from SAE International.

Table C.1: OHA Worksheet Categories

Hazard ID	Hazard Description	Cause	System State
Alpha-numeric identifier (under 10 characters)	Any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment	The origin of a hazard	An expression of the various conditions, characterized by quantities or qualities, in which a system can exist. The identified system state is the one that most expresses the identified hazard, or the system state that would express the highest risk.

Controls:

Controls	Control Justification
Any means currently reducing a hazard's causes or effects	A justification for each control, indicating its effect on the identified hazard's causes or effects

Severity and Safety Objectives:

Effect	Severity	Severity Rationale	Safety Objectives/ Requirements
The real or credible harmful outcome that has occurred or can be expected if the hazard occurs in a defined system state	The consequences or impact of a hazard's effect or outcome in terms of degree of loss or harm	Explanation of how severity was determined	Description of the baseline acceptable risk for the hazard

3.3 Allocation of Safety Objectives and Requirements

The operational objectives and safety requirements identified in the OHA form the basis for assessing the safety of any developed solution. For OSAs conducted across multiple domains, the Allocation of Safety Objectives and Requirements (ASOR) allocates the safety objectives and requirements to the service level (e.g., Air Traffic Services or Flight Standards Service), develops and validates risk mitigation strategies shared by multiple organizations, and allocates safety requirements to those organizations. For OSAs conducted within a domain or at a distributed level, the ASOR allocates the mitigations and controls to their respective disciplines (e.g., equipment specification, procedure requirements, training, logistics, and maintenance).

In the ASOR, safety requirements are developed to achieve the safety objectives identified in the OHA. Safety objectives and safety requirements must then be allocated (1) to the CNS/ATM system elements that provide the functional capability to perform the service and (2) to the stakeholders in control of or responsible for each of the elements. Safety objectives and requirements must be further synthesized into the appropriate standards and specifications, which are used by the FAA/ATO to ensure that systems are compliant.

The ASOR uses the safety objectives and requirements developed and derived from the OHA to develop a strategy that considers procedural and architectural mitigations. The set of safety requirements to meet the objectives are allocated to the various ground and/or airborne CNS/ATM systems.

3.3.1 ASOR Development Process

The ASOR development process is described below.

3.3.1.1 Identify Shared Risk Mitigation Strategies

Identify the relationships between CNS/ATM solution failures, procedural errors, and their effects on air traffic services and the hazard. Include the identification of common cause failures and errors occurring among elements of the solution. Identify risk mitigation strategies that are shared by multiple elements of the CNS/ATM solution, including the mitigation of effects from common cause failures and errors occurring across solution elements. CNS/ATM solution mitigation includes architectural and procedural aspects of the solution as well as environmental mitigation and related candidate safety requirements identified in the OHA.

3.3.1.2 Allocate Safety Objectives and Requirements

Recommend the allocation of the safety objectives and safety requirements, including safety requirements from environmental mitigation, to elements of the CNS/ATM solution. (Note: These requirements should be included in the pPRD.) The allocations may require updates based on feedback from other processes (e.g., safety requirements from other OSAs or Memoranda of Understanding between the ATO and Aviation Safety). Allocations may also require updates based on an organization's rejection of responsibilities initially assigned by the OSA. Understanding the interactions of air traffic procedures and airspace characteristics assists in the identification of failures, errors, and combinations of both that contribute significantly to the hazards identified in the OHA.

3.3.1.3 Share Safety Objectives and Coordinate Safety Requirements

Safety objectives and requirements must be coordinated and promulgated to the appropriate program artifacts, including the pPRD.

3.4 Assemble the OSED, OHA, and ASOR as an OSA and Prepare It for Approval

OSAs must be approved in accordance with the version of the SMS Manual cited in the approved PSP. (Note: The PO must submit OSAs that support NAS acquisitions to Safety and Technical Training (AJI) Policy and Performance, AJI-3, for approval.[8]) The PO must also upload OSAs to the Safety Management Tracking System (SMTS) per the instructions in the SMTS User Manual.

4 Use of Results

The results of the OSA may be used as inputs to various documents.

4.1 Preliminary Requirements

Controls and safety requirements identified through the OSA process must be included in the pPRD. The pPRD must include a requirement for DALs. If a preliminary requirement is not included in the pPRD, it must be separately documented, such as in new/modified ATC procedures, changes to the Code of Federal Regulations, and training.

4.2 SRM Documents

The OSA serves as a foundational SRM document for subsequent SRM documents that the PO creates as the solution is further developed (e.g., Comparative Safety Assessment, Preliminary Hazard Analysis, or System Hazard Analysis / Sub-System Hazard Analysis).

8. ANG is the review and acceptance authority for all OSAs prepared for the Concept and Requirements Definition phase of the AMS lifecycle; however, an OSA is not required for entrance into this phase.

4.3 Safety Requirements Verification Table

The Safety Requirements Verification Table, which is typically documented in the System Safety Assessment Report, contains all of the safety requirements identified, starting with the origin of the requirements (including those identified in the OSA).

Appendix D
Conducting and Documenting a Functional Hazard Assessment

Conducting and Documenting a Functional Hazard Assessment

1 Background

1.1 Description

A Functional Hazard Assessment (FHA) is a predictive technique that identifies every expected function of a system and considers the hazards that may result when each function fails in every possible way. The Program Office (PO) may conduct an FHA during the Concept and Requirements Definition phase of the Federal Aviation Administration (FAA) Acquisition Management System (AMS) lifecycle to identify credible operational safety effects through the methodical assessment of system or sub-system functions and failure conditions. An FHA does not determine causes of the hazards but rather focuses on the consequences and corresponding severities. A guiding principle of the FHA is that if safety requirements are added at the functional level early in the system development process, then the design of the system will be more stable from a safety perspective, and the cost of implementing safety mitigations will be reduced. The FHA also provides a foundation for the safety program to scope additional safety analyses/assessments.

The FHA is an engineering-oriented assessment. To conduct an FHA, before a Safety Risk Management (SRM) panel is held, the PO must convene a technical- or engineering-oriented workgroup to review the Functional Analysis (FA), preliminary Program Requirements Document (pPRD) (if available), Enterprise Architecture (EA) artifacts, and other inputs. In completing the FHA, the workgroup should define system functions, identify likely functional hazards, and discuss mitigations and solutions. This work will enhance the safety program's future safety-related efforts. The FHA also assists any stakeholders participating in subsequent SRM panels (e.g., an Operational Safety Assessment (OSA)) who may not have a sufficient technical understanding of the system or change under analysis to fully participate in its functional definition. Subsequent SRM panels must then translate the functional hazard effects into operational effects to assess any operational impacts.

2 FHA Definitions

2.1 Function

A function is a specific or discrete action (or series of actions) that must be performed to achieve a desired service objective or stakeholder need. Functions are used to develop requirements, which are then allocated to solutions in the form of a physical architecture. A function occurs within the service environment and is accomplished by one (or more) solution element composed of equipment (e.g., hardware, software, and firmware), people, and procedures to achieve system operations.

2.2 FA

The FA translates the service needs identified in the Shortfall Analysis and Next Generation Air Transportation System Midterm Concept of Operations (ConOps) into high-level functions that must be performed to achieve the desired service outcome. This process then decomposes high-level functions into lower-level sub-functions. The outcome is a functional architecture that serves as a framework for developing requirements and the subsequent physical architecture. It is important that the definition of functions focuses on what the new capability will do rather than how the service will be provided.

2.3 EA Artifacts

EA artifacts include the following:

- **Systems Functionality Description (SV-4):** The SV-4 is an EA artifact that illustrates functions performed by systems and the data flows among system functions. The results of the FA directly contribute to the development of the SV-4 artifact.
- **Operational Activity Model (OV-5):** The OV-5 describes the operations that are conducted in meeting a business or mission goal.

3 FHA Methodology

3.1 Overview

An FHA is a methodical approach for identifying credible operational safety effects through the assessment of system or sub-system functions and failure conditions. The FHA identifies and classifies the system functions and safety hazards associated with functional failure or malfunction. It identifies the relationships between functions and hazards, thereby identifying the safety-significant functions of the system as well as the hazards associated with those functionalities. This identification provides a foundation for the safety program to scope additional safety analyses/assessments.

Requirements and design constraints are recommended for inclusion in the system specifications to eliminate or reduce the risk of the identified hazards once the system is successfully implemented.

3.2 FHA Inputs

The following are some of the inputs to an FHA:

- ConOps
- Operational context description (typically found in the ConOps)
- EA artifacts
- System architecture data (e.g., inputs, outputs, and flow of functions)
- Policy and standards
- Interface control documents
- Legacy system documentation
- FA
- pPRD
- Operational requirements
- Maintenance and support concept

3.3 FHA Process

Systematically, the FHA identifies:

- The functions, purposes, and behaviors of a system.
- Considerations of how the system fails (e.g., when can the failure conditions occur? In what operational environment will these failures be present?). Consider the following hypothetical failure modes. (Note: Additional failure types may be identified through system reports and subject matter expertise.)

- **Fails to operate:** A function does not occur/perform when given the appropriate input.
- **Operates early/late:** A function performs earlier or later than it should.
- **Operates out of sequence:** A function occurs before or after the wrong function; a function occurs without receiving the appropriate inputs.
- **Unable to stop operation:** A function continues even though the thread should move onto the next function.
- **Degraded function or malfunction:** A function does not finish or only partially completes; a function generates improper output.

- The impact or effects that failures may have (e.g., does the functional failure constitute a hazard?).

4 FHA Output

The output of the FHA provides inputs to the OSA and the Preliminary Hazard Analysis and plays a major role in determining the Development Assurance Levels for the system.

5 FHA Approval

The FHA is not a document required by either the AMS or the Safety Risk Management Guidance for System Acquisitions.[1] However, its findings may be useful as an input to subsequent SRM panels. FHA approval should be performed in accordance with PO work processes.

1. Although desirable to conduct, an FHA is not required as a stand-alone assessment. However, it may be required as part of the PO's system, software, and electronic hardware development assurance process.

Appendix E
Conducting and Documenting a Comparative Safety Assessment

Conducting and Documenting a Comparative Safety Assessment

1 Background

1.1 Description

Unless specifically waived in an approved Program Safety Plan, the Program Office (PO) must conduct a Comparative Safety Assessment (CSA).

A CSA provides management with a level comparison of all the identified potential safety hazards associated with meeting competing sets of operational requirements for alternate solution approaches and architectures. It provides a detailed safety risk assessment for each proposed investment alternative that is being considered by defining the initial risk and the predicted residual risk of each proposed alternative.

A CSA is an extension of an Operational Safety Assessment (OSA). Whereas an OSA defines the target level of likelihood required to achieve an acceptable level of safety irrespective of a solution, a CSA provides an estimation of the potential safety risk associated with each proposed solution alternative. Some alternatives that were not viable may have been discarded prior to this point. The remaining alternatives must now be complete, diverse, and technically viable.

The CSA uses the top-level Functional Analysis (FA) that was developed before the OSA. This FA is then decomposed at least one more level to further expand the Preliminary Hazard List (PHL)[1] produced in the OSA. If an FA has not been previously developed, the PO may need to develop one as an input to the CSA. If an OSA has not been previously conducted, then the PO may need to develop a PHL in the CSA.

The alternatives assessed may range from the reference case[2] of maintaining the status quo to implementing new designs, procedures, or program operational changes. The CSA determines the acceptability of each alternative from a safety risk perspective to allow informed and data-driven decisions to be made by Federal Aviation Administration (FAA) management. Other considerations in making a final alternative decision include cost, schedule, outside interdependencies, and training; however, they are not within the scope of a CSA. Those considerations are discussed in the Final Investment Analysis Plan or in Business Case Reports. CSAs are typically conducted internally by the PO with members from the Program Safety Team (PST)[3] and other subject matter experts serving on a Safety Risk Management (SRM) panel.

The Initial Investment Decision (IID) is the point at which the Joint Resources Council (JRC) approves or selects the best alternative that both meets the required performance and offers the greatest value to the FAA and its stakeholders. To support the IID, the PO must complete a

1. The concept of the PHL is explained in the Air Traffic Organization Safety Management System Manual.

2. Before differences brought about by a proposed change may be fully understood, the “reference case” must be stated. The reference case provides conditions as they are, or would become, if the proposed change is not accepted. The reference case provides a contextual basis to see and compare differences over time.

3. A PST is a resource provided by the PO to support the safety efforts of an acquisition throughout the FAA Acquisition Management System lifecycle. The PST is supported by a safety case lead from the Safety and Technical Training (AJI) Safety Engineering Team, AJI-314.

CSA and, through Safety and Technical Training (AJI),[4] inform the JRC of the safety risk acceptability of each alternative.

1.2 Overview

Figure E.1 provides an overview of the CSA development process.

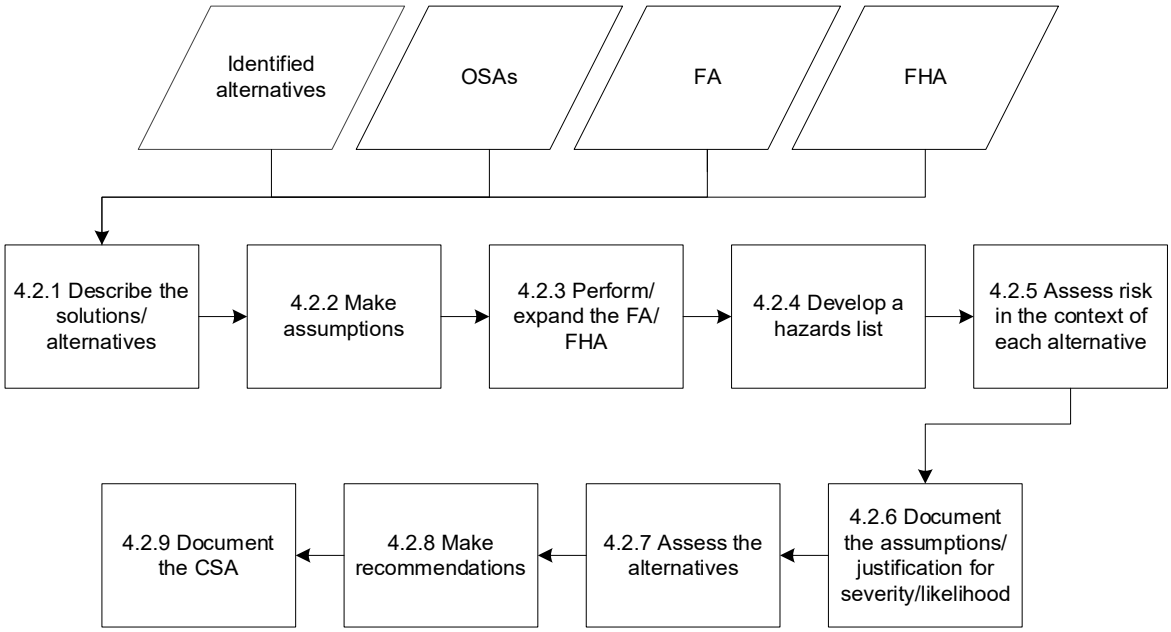

Figure E.1: The CSA Development Process

2 Initial Inputs

The following are examples of inputs to the CSA.

2.1 Identified Alternatives

If possible, investment analyses should bring at least three diverse, yet technically viable alternatives forward for selection of a preferred solution alternative. The reference case is typically one of the alternatives assessed. The reference case is not always a “do-nothing” scenario, since many legacy program activities may already be in place and may go through some default evolution during the required implementation time of the alternative solutions. Therefore, potential safety consequences stemming from letting an existing system continue without further investment and without the targeted new capability must be fleshed out. This should address whether the targeted new capability is an improvement or a deterioration to the existing system.

2.2 OSAs

OSAs previously conducted for the Investment Analysis Readiness Decision may provide relevant information concerning safety hazards, causes, solution states, effects, and severity assessments to the CSA. Using these as inputs to the CSA, the likelihood of each

4. Policy and Performance, AJI-3, is responsible for this.

hazard/cause/effect must be determined and matched with a severity rating. Differences among alternatives should begin to emerge, which could impact the combinations of cause/effect, severity, and likelihood ratings associated with each hazard.

2.3 FA

An FA, as described in the FAA Systems Engineering Manual, is used to examine the functions and sub-functions of a system solution that may accomplish the system's operation or mission. An FA describes what the system does (not how it does it) and is conducted at a level needed to support later synthesis efforts. Products from the FA, such as the Functional Flow Block Diagram and N^2 diagram (although other techniques may be used to diagram system functions), are further matured as the system's lifecycle progresses and may be used when developing the CSA. If the alternative solutions are sufficiently diverse, then the functional architectures (as yet solution agnostic) begin to exhibit significant differences that affect safety risk, making the CSA valuable. Should no difference in safety risk be determined, the CSA no longer helps to distinguish a preferred alternative, which leaves outside Business Case factors as sole determinants.

Note: The FA involves an iterative process that results in an increasingly refined functional architecture. The functional architecture cannot be finalized until the system's final requirements are completely defined. This is most likely after the CSA is performed.

2.4 Functional Hazard Assessment

A Functional Hazard Assessment (FHA) is a methodical approach to identifying credible operational safety effects through the assessment of system or sub-system functions and failure conditions. See Appendix D of the Safety Risk Management Guidance for System Acquisitions for further information.

3 CSA Development Process

3.1 Describe the Solutions/Alternatives

Describe the solutions under study in terms of the 5M Model, per the Air Traffic Organization Safety Management System (SMS) Manual. At this point, a number of different architectures and alternatives have been identified to meet the operational requirement. Describe each alternative in sufficient detail to ensure the audience can understand the proposed solution.

3.2 Make Assumptions Only If Specific Information Is Not Available

As necessary, make assumptions that are conservative in nature and clearly identified. Make them in such a manner that they fairly distinguish among the alternatives which aspects do or do not adversely affect the safety of the solution.

3.3 Perform/Expand the FA/FHA

Perform an FA/FHA (or expand the ones previously developed). Attempt to match similar and unique causes associated with each hazard into a firm list of unique events that may be adequately addressed by existing functions or by postulating new low-level system functions. This analysis results in complete sets of hierarchical functions that alternative system solutions must perform.

Look for matches between system function and mitigation of all causes (within system bounds). Organize causes that fall beyond system bounds into assumptions and constraints for coordination with external National Airspace System (NAS) entities. Though all such external

dependencies may be noted, it may not be possible to address them within the bounds of this system.

Analyze all external causes that cannot be mitigated within system bounds for faulty assumptions that may invalidate the efficacy of the best solution that could be engineered. Adjust concepts as needed until a good fit is obtained between hazard causes that can be mitigated within this system boundary and operational plans for reaching adequacy of every listed (known) external constraint.

Decide which alternative solutions remain viable after a cursory look at safety. Discard any potential solution "fragments"[5] that inadequately address safety concerns.

3.4 Develop a Hazards List

From the FA and solution description, refine and expand (as necessary) the partial PHL developed in the OSA (assuming an OSA was conducted). If a partial PHL was not previously compiled, then develop one as described in the SMS Manual. Carry over any valid OSA-identified hazards / causes / solution states / severity ratings to the CSA. If any OSA hazards need to be deleted or modified in the CSA, provide a supporting rationale as to why this must be done. Table E.1 presents a sample hazard list that has been expanded/modified from an OSA.

Table E.1: CSA Hazards List

ID	Hazard	Disposition for CSA	Validity/Rationale
OSA TFDM-1	Loss of all system functionality	Becomes TFDM-1	Valid hazard
OSA TFDM-2	Loss of electronic flight display	Becomes TFDM-2 with enhanced wording	When updated, needed hazard
OSA TFDM-3	Incorrect flight data display	Becomes TFDM-3	Valid hazard
OSA TFDM-4	Controller fails to pass and/or edit electronic flight strips in a timely and efficient manner	Deleted	Invalid hazard: SRM panel believes the system fails, not the controller
TFDM-X	(To be determined)	Newly identified	N/A

3.5 Assess Risk in the Context of Each Alternative

Evaluate each hazard-alternative combination (including the reference case) for risk differences using the definitions and principles contained in the SMS Manual. Use the hazard severity in the context of the worst credible conditions. Remember, severity can and should be defined independently of the likelihood of occurrence. Evaluate the likelihood of the hazard conditions resulting in an event at the highest level of severity and not simply the probability of any hazard occurring.

3.6 Document the Assumptions and Justifications

Clearly define which adverse events are to be tracked as the best indicators of safety. Identify how to measure adverse events and provide any baseline measures prior to the proposed

5. NAS services may be composed of many cooperating parts or "solution fragments" in the form of federated systems, sub-systems, or services, all of which must be efficiently orchestrated to achieve some desired operational capability outcome for users. Solution fragments accomplish nothing individually without the rest of the NAS "system of systems" to provide benefits to end users.

change, if known. Trace through causes and solution states to arrive at a means of distinguishing those measures that quantitatively (or only qualitatively) support declarations of severity by the SRM panel. In the early stages of SRM for alternative concepts, there are occasionally solution fragments and less than fully defined systems, making it difficult to assign specific severity and likelihood ratings. Document assumptions and justifications for how the severity and likelihood for each hazard condition were determined. Describe whether the alternatives are detailed enough at this stage in development to draw meaningful conclusions about their differences with regard to safety. If additional information is required, describe when and how any deferred analysis reaches a definitive answer, if possible. Describe any new data collection methods required and identify future decision points at which important measures are likely to be available.

3.7 Assess Each Alternative from a Safety Perspective

Assess the acceptability of the safety risk associated with the implementation of each alternative under consideration. Document the assessments using Table E.2. (Note: Each alternative assessed has its own table.) Summarize any similarities and note any significant differences. Explain the level of confidence with the outcome by determining a rudimentary level of precision with regard to the possible breadth of range of values that the SRM panel expressed.

Table E.2: CSA Worksheet Categories

Hazard ID	Hazard Description	Cause	System State
Alpha-numeric identifier (under 10 characters)	Any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment	The origin of a hazard	An expression of the various conditions, characterized by quantities or qualities, in which a system can exist

Controls:

Control	Control Justification
Any means currently reducing a hazard's causes or effects	A justification for each control, indicating its effect on the identified hazard's causes or effects

Initial Risk:

Effect	Severity	Severity Rationale	Likelihood	Likelihood Rationale	Initial Risk
The real or credible harmful outcome that has occurred or can be expected if the hazard occurs in the defined system state	The consequences or impact of a hazard's effect or outcome in terms of degree of loss or harm	Explanation of how severity was determined	The estimated probability or frequency, in quantitative or qualitative terms, of a hazard's effect or outcome	Explanation of how likelihood was determined	The composite of the severity and likelihood of a hazard, considering only controls and documented assumptions for a given system state

3.8 Assess Development Assurance Risk

Consider the architectures of the alternatives, the different components, and their Development Assurance Levels (DALs). Developing all components to the highest DAL is expensive and spreads the developer's resources across the entire project. However, partitioning the components may permit different DALs, limiting the most severe functions to one component. Other functions can be assigned lower DALs, thus conserving resources. Also, if the different implementations are from different vendors, consider their experience with the DAL standard; inexperience may add additional risk.

3.9 Establish Safety Requirements and Predict Residual Risks

For each alternative, establish:

- Preliminary safety issues for tracking in the future;
- Needs, which may become requirements when validated;
- Missing functional requirements needed to turn solution fragment(s) into complete and viable solutions; and
- Predicted residual risk levels based on potential and achievable performance minima should this alternative be selected, designed, fabricated, tested, fielded, and logistically supported for its full lifecycle.

At this point, the CSA may only lay the groundwork to better define a preferred alternative (as yet unselected) that will be better detailed in the Preliminary Hazard Analysis (PHA). Again, some aspects of relative difference among alternatives may be apparent even if absolute measures of each alternative's suitability against the reference case may not be known.

Intelligently discount and drop out similar unknowns deemed "equal" across each of the alternatives, leaving the known differences as key points of distinction. When completed, the CSA positively impacts the decision-making process by helping to discount several lesser alternatives, indicating one preferred alternative on the basis of clear differences in predicted residual risk. Alternatively, the CSA may return a "no discernible difference" result, leaving subsequent IIDs to be made on the basis of outside Business Case factors. Use Table E.3 to tabulate results. (Note: Each alternative assessed has its own table.)

Table E.3: Safety Requirements and Residual Risks

Hazard ID	Initial Risk	Safety Requirement Description	Predicted Residual Risk	Predicted Residual Risk Rationale
Alpha-numeric identifier (under 10 characters)	The composite of the severity and likelihood of a hazard, considering only controls and documented assumptions for a given system state	A planned or proposed means to reduce a hazard's causes or effects	The risk that is estimated to exist after the safety requirements are implemented or after all avenues of risk mitigation have been explored	If necessary, any additional explanation needed to help the reader understand how the predicted residual risk was determined

3.10 Make Recommendations Based on the Data in the CSA

For decision-making purposes, compare the results of the safety risk assessment of each alternative considered. Compile the results in Table E.4. (Note: Not all hazards may apply to each alternative assessed. Enter "N/A" in Table E.4 when appropriate.) Ensure the decision makers can clearly distinguish the safety merit of each alternative. Prepare an executive summary that clearly states whether the CSA finds all alternatives alike or whether one or two particular alternatives are clearly superior to others on the basis of safety risk.

Note: The cost of implementing the recommended hazard mitigations identified for each alternative is not a CSA consideration; the safety acceptability of each alternative is the only consideration.

Table E.4: Comparison of Safety Assessments

Alternative	Alternative Description	Risk Rating					
		Hazard 1 Name	Hazard 2 Name	Hazard 3 Name	Hazard 4 Name	Hazard 5 Name	Comments
1							
2							
x							

3.11 Document, Assemble, and Prepare the CSA for Approval

CSAs must be approved per SMS Manual policy. The PO must upload the CSA to the Safety Management Tracking System (SMTS) following the instructions in the SMTS User Manual.

It is particularly important that the PO enters hazards and the safety requirements from the CSA into SMTS so that the PHA (for the eventual preferred alternative) and subsequent verification and validation activities may be tracked once an alternative is down-selected.

4 Use of Results

The results of the CSA may be used as inputs to the items described below.

4.1 Preparing/Revising the Program Requirements Document

Controls from the reference case and generic safety requirements that are identified through the CSA process for each selected alternative (as yet solution agnostic) must be included in the Program Requirements Document (PRD). Related changes by alternative analyses must be separately documented. These changes include preliminary requirements from interdependent investments, new/modified air traffic control procedures, compliance with updates to the Code of Federal Regulations, and lifecycle-integrated logistics support (e.g., maintenance and training). At this stage, the initial PRD (iPRD) defines the program's needs and requirements at a high level.

4.2 Establishing the DALs

The system-level DALs for each alternative (if applicable) are reassessed in the CSA. Note: The DALs may differ among the investment alternatives assessed.[6]

6. The DALs for the eventually selected alternative must be included in the iPRD and the initial Implementation Strategy and Planning Document prior to the Final Investment Decision.

4.3 Preparing SRM Documents

The output of the CSA should be used as an input to other SRM documents, particularly a PHA,[7] as the capability/solution alternative pros and cons are debated after the IID.

4.4 Preparing/Revising the Safety Requirements Verification Table

The Safety Requirements Verification Table (SRVT) contains all of the safety requirements identified, starting with the origin of the requirement, and should include the requirements identified in the CSA. The final SRVT is not required until the System Safety Assessment Report is prepared.

7. A PHA is best compiled after the alternatives are evaluated and a single alternative is selected as the best option. The PHA is conducted after the CSA and before the Final Investment Decision.

Appendix F
Conducting and Documenting a Preliminary Hazard Analysis

Conducting and Documenting a Preliminary Hazard Analysis

1 Background

1.1 Description

For system acquisitions, the Preliminary Hazard Analysis (PHA) is a broad initial hazard identification process conducted by the Program Office (PO) during the Investment Analysis phase of an acquisition. It is a systematic hazard analysis of the early system hardware and software design, the environment in which the system will exist, and the system's intended use or application. It is primarily used to identify potential hazards and associated high-level safety requirements. The PHA is conducted early in the life of a system; timely identification and incorporation of requirements may save time and money later if hazards and associated safety requirements that could require a major system redesign are subsequently identified.

The output of the PHA is used to develop detailed system safety requirements, which may assist with preparing performance and design specifications. In addition, the PHA is often a precursor to more detailed safety risk analyses (e.g., System Hazard Analysis or Sub-System Hazard Analysis), as additional safety analyses are generally required to more fully understand and evaluate safety hazards identified by a Safety Risk Management (SRM) panel. Per the Federal Aviation Administration (FAA) Acquisition Management System (AMS), approval of the PHA is a requirement for consideration at the Final Investment Decision.

At the time a PHA is conducted, there are few, if any, fully developed system specifications and little or no detailed design information. Therefore, this analysis relies heavily on the knowledge of Subject Matter Experts (SMEs). If these SMEs do not participate on the SRM panel preparing the PHA, or if the system is a new technology having little or no early operational history, the results of the PHA will reflect the uncertainty of the panel in many of its assessments and assumptions.

A PHA may be used as a complete safety risk analysis of some systems. This possibility depends both on the complexity of the system and the objectives of the analysis. This is determined by the PO at the Safety Strategy Meeting and is reflected in an approved Program Safety Plan (PSP).

The PHA is often conducted in-house by the PO. However, if contracted out, an appropriate Data Item Description must be included as a part of the contract.

2 Conducting a PHA

2.1 Overview

The PHA follows the DIAAT process (**D**escribe the System, **I**dentify Hazards, **A**nalyze Risk, **A**ssess Risk, **T**reat Risk) identified in the Air Traffic Organization Safety Management System (SMS) Manual by identifying potential safety hazards, ranking them according to their severity and likelihood ratings, and translating these potential hazards into high-level system safety controls (see Figure F.1). Steps 1 through 3 are conducted by the change proponent (typically the PO); the remaining steps are conducted by the SRM panel.

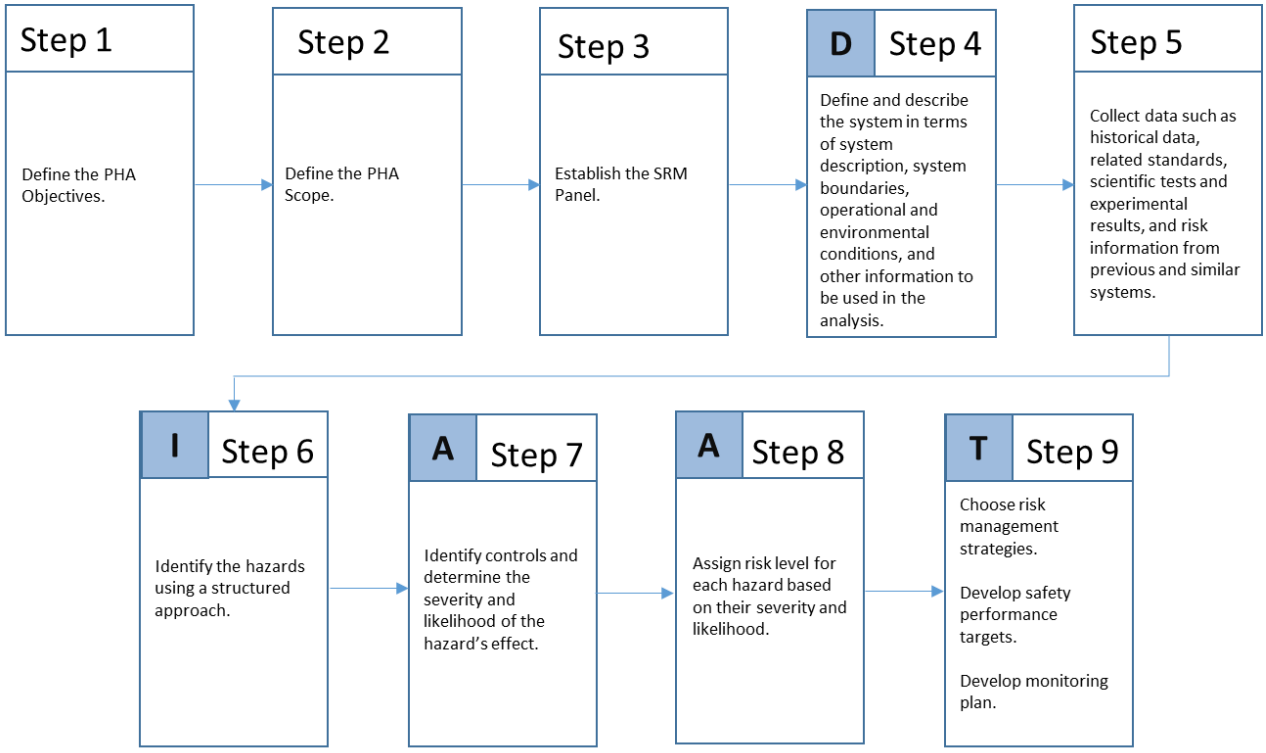

Figure F.1: PHA High-Level Process

2.2 Hazard Analysis Techniques

The SMS Manual and the FAA Systems Engineering Manual describe various hazard analysis techniques that may be used in developing the PHA. These techniques include:

- Function failure analysis,
- Event tree analysis,
- Failure mode and effect analysis,
- Fault tree analysis,
- Cause-consequence diagram, and
- "What if" analysis.

2.3 Inputs

Typical inputs to a PHA include:

- **System Description:** A description of the system under development and the context in which it is to be used, including layout drawings, process flow diagrams, and block diagrams. It also includes system functions within the architecture and proposed changes.
- **Safety Data:** Historical hazard data (including lessons learned from other systems) that allow for the incorporation of experience gained from previous operation of the same system or similar systems. Potential data sources are listed in the SMS Manual.

- **Functional Analysis (FA):** An expansion of the FAs conducted to support the Operational Safety Assessment (OSA) or Comparative Safety Assessment (CSA) conducted earlier in the AMS lifecycle.
- **Functional Hazard Assessment:** A methodical approach to identifying credible operational safety effects through the assessment of system or sub-system functions and failure conditions.
- **Hazard Checklist:** A list of the causes of safety incidents with the same or similar equipment.
- **Customer Requirements:** Any pre-existing requirement specifications and concept documents.
- **Regulatory Requirements:** Constraints imposed by regulatory agencies.
- **Previously Conducted Safety Assessments/Analyses:** Any relevant information from safety assessments/analyses (e.g., OSAs, CSAs, or Safety Collaboration Team / Office of NextGen studies) already conducted.
- **Development Assurance Levels (DALs):** Preliminary Functional DALs (FDALs) that may have been established based on previously conducted assessments/analyses.

The PHA is an SRM document that must follow the format outlined in the SMS Manual. The Hazard Analysis Worksheet (HAW) and the monitoring plan are essential elements of the PHA. The components of the HAW and the monitoring plan are described in the SMS Manual.

3 Preparation for Approval

PHAs must be reviewed in accordance with the Safety and Technical Training (AJI)–facilitated peer review process and approved by the Director of Policy and Performance, AJI-3, per the guidance given in the Safety Risk Management Guidance for System Acquisitions and the SMS Manual.

In addition, the PO must enter into the Safety Management Tracking System the safety hazards and requirements identified in the PHA so that subsequent verification and validation activities may be tracked and monitored.

4 Use of Results

The PHA should help the PO to:

- Identify and develop safety requirements to be included in the final Program Requirements Document.
- Highlight significant safety risks and issues.
- Recommend additional safety risk analyses/assessments. As suggested by the name, the PHA is conducted in an early phase of a project. The insights gained from the PHA help determine which, if any, additional safety risk analyses should be conducted and serve as input to these more detailed analyses. The recommendations for additional analyses must be reflected in an approved PSP.

- Develop/refine FDALs using SAE Aerospace Recommended Practice (ARP)[1] ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*, or equivalent processes and allocate them to software and electronic hardware Item DALs.
- Develop a hazard monitoring and tracking plan.
- Use the PHA as an input into subsequent safety analyses.

5 Updating the PHA

If any subsequent analyses identify a safety hazard that cannot be traced back to one identified in the PHA, the PO must update the PHA and resubmit it for approval by AJI-3.

1. An ARP is a guideline from SAE International.

Appendix G
Conducting and Documenting a Sub-System Hazard Analysis

Conducting and Documenting a Sub-System Hazard Analysis

1 Background

1.1 Description

Conducting a Sub-System Hazard Analysis (SSHA) is an important part of system safety.[1] It is performed in the early stages of the Solution Implementation phase once system design details are known. The SSHA determines how operational or functional failures of components (or any other anomalies) may adversely affect the overall safety risk associated with possible outcomes of the system being used in the National Airspace System. It addresses the safety in sub-systems by conducting a detailed analysis that identifies hazards and recommends solutions.

The SSHA takes the previously identified hazards that originated in the Preliminary Hazard Analysis (PHA) and any other sources; considers the sub-system design and architecture; and refines those hazards through analytical selection, decomposition, and traceability. Sometimes this analysis uncovers new hazards that manifest because of an implementation choice. If the SSHA identifies a safety hazard that is new or cannot be traced back to a hazard identified in the PHA, the Program Office (PO) must update the PHA and re-submit it for approval by the Director of Safety and Technical Training (AJI) Policy and Performance, AJI-3.

The SSHA focuses on failure modes as they contribute to hazards at the sub-system level and investigates the detailed interfaces between components for possible conditions leading to hazards. In addition, the analysis focuses on component and equipment failures or faults and human errors that establish a hazard due to the functioning of the sub-system. The analysis is completed by reviewing design drawings, engineering schematics, and specifications. As the system and related sub-systems are further defined and system design changes (including software design changes) are implemented, the system developer must revise the SSHA as necessary.

2 Process Overview

The SSHA process is iterative, beginning as a preliminary analysis early in the design development and then maturing to eventually document the state of the final system. Early in development planning, the SSHA may:

- Develop system safety design constraints;
- Identify specific system safety requirements; and
- Devise system safety test plans and testing requirements.

As the design progresses, the SSHA may:

- Ensure that the method for design, requirements specification, implementation, and corrective action planning does not impair or increase the safety risk associated with the sub-system;
- Evaluate any new safety hazards introduced into the system;
- Design and analyze the human-computer interface;

1. For the sake of simplicity, a “system” is considered to be a whole that cannot be divided into independent parts without losing its essential characteristics. A “sub-system” is a constituent part of a system that performs a particular function.

- Develop safety-related information for operations, maintenance, and training manuals; and
- Evaluate whether potential changes to the hardware or software could affect safety.

Sub-systems may be a single media type (e.g., electronic, software, or mechanical). In addition, there may be mixed-media sub-systems such as embedded software-hardware systems or electromechanical actuators that require a more integrated SSHA. In either case, the human is considered a component that both receives inputs and initiates outputs within a sub-system.

If hazards are not identified and corrected during the design process, then they might not be identified and corrected later when the sub-system designs are frozen, and the cost of making a change could significantly increase.

Due to the complexity of the SSHA, the analysis is usually identified in a procurement specification and conducted by the system developer. If so, the PO must include the need to conduct an SSHA as a contractual requirement. An appropriate Data Item Description must be included as part of the contract. The PO must also require that Safety Risk Management (SRM) panels be conducted. Further, if facilitated or conducted by the developer, the SRM panels must include subject matter experts, particularly those with an operational perspective. The Federal Aviation Administration (FAA) must actively review and be able to modify/comment on the safety analysis documentation as it is being prepared by the developer and not just at its final delivery. The developer must incorporate any valid comments received from the government's peer review process

The Program Management Organization (AJM) must approve the SSHA by the In-Service Decision (ISD) review.

2.1 System Aspects of Analysis

The following sections of the Safety Risk Management Guidance for System Acquisitions may be relevant to the SSHA:

- Section 2.3.2.1.4, System Development Assurance (for the Investment Analysis Readiness Decision)
- Section 2.3.3.1.2, System Development Assurance (for the Initial Investment Decision)
- Section 2.3.4.1.2.1, System Development Assurance (for the Final Investment Decision);
- Section 2.3.5.1.3, System Development Assurance (for the ISD)
- Section 9.4, System Development Assurance
- Appendix A, Guidance for Preparing and Implementing Program Safety Plans, Section 3.1.3, Identify Developmental Assurance Requirements
- Appendix B, Overview of the System Safety Program Plan, Section 2.3.7, Development Assurance Activities

3 Preparing the SSHA

3.1 Initial Inputs

Figure G.1 shows some possible inputs to the SSHA.

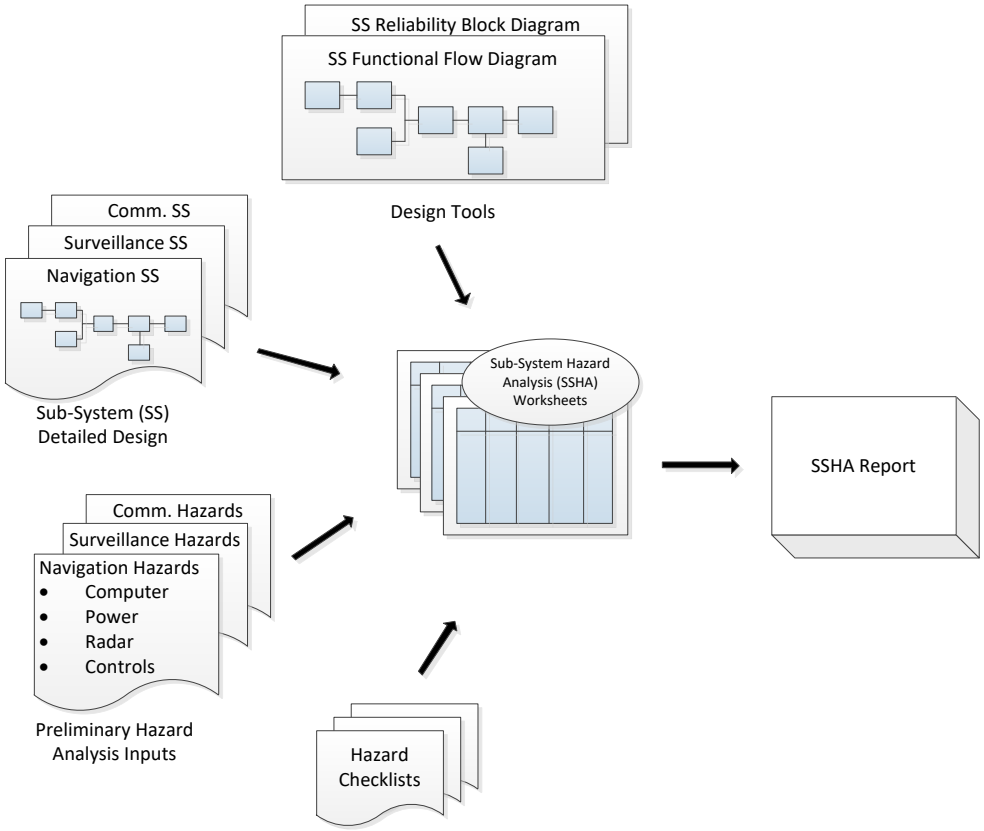

Figure G.1: Inputs to the SSHA

3.2 Hazard Analysis Techniques

Refer to the Air Traffic Organization Safety Management System Manual and the FAA Systems Engineering Manual for descriptions of various hazard analysis techniques that may be used in developing an SSHA. These techniques include:

- Function failure analysis,
- Event tree analysis,
- Failure mode and effect analysis,
- Fault tree analysis,[2]
- Cause-consequence diagram use, and
- "What if" analysis.

2. Fault tree analyses alone are incomplete and do not directly provide useful information. The utility of fault trees comes from the cut and path sets they generate, the analysis of the cut and path sets for common cause failures, and the independence of failures/faults. Fault trees are good for analyzing a specific undesired event (e.g., rupture of a pressure tank) and can find sequential and simultaneous failures but are time-consuming and expensive.

3.3 Conducting the SSHA

The SSHA is essentially a PHA conducted at the sub-system level. It is recommended that the SSHA be led by safety engineers with technical proficiency rather than design or system engineers. This is to ensure that the analysis remains a tool to identify hazards and safety issues associated with the design and functional operation of the system, not a defense of the existing design. Design or system engineers may have difficulty looking away from the sub-system and/or system designs that they created. The safety engineer must provide a unique, non-parochial view that focuses on potential hazards.

3.4 Reviewing and Approving the SSHA

The PO must facilitate a peer review of the SSHA and ensure that a copy is sent to the AJI safety case lead for review and comment. The final document must be approved per AJM guidance. The PO must upload the SSHA to the Safety Management Tracking System (SMTS) per the instructions in the SMTS User Manual.

3.5 Preparing and Revising the Safety Requirements Verification Table

The Safety Requirements Verification Table (SRVT) must contain all of the safety requirements identified (existing, validated, and recommended),[3] starting with the origin of the requirement, and must include those safety requirements identified in the SSHA.

4 Other Considerations

4.1 Software

When the software to be used in conjunction with the sub-system is developed under a separate software development effort, the system developer performing the SSHA must monitor, obtain, and use the output of each phase of the formal software development process to evaluate the software contribution to the SSHA. Identified hazards that require mitigation action by the software developer must be reported to the PO to request that appropriate direction be provided to the developers.

Until this point, the SRM process was conducted without any specific details about implementation and thus had to rely on assumptions about how the system would behave. As part of the sub-system, the software is addressed in the SSHA by the system developer. Individuals performing an analysis on the system may not necessarily be experts in software behavior. In addition, the software developer may be a subcontractor to the system developer. Thus, it is critical that the SSHA process address how the software analysts and system analysts communicate and understand each other. The software aspects of hazard analysis must ensure that (1) the people doing the safety analysis know enough about the software implementation details to ensure the safety analysis is still valid and (2) these people are not surprised by an unexpected implementation method. Although the term “software hazard analysis” is sometimes used, the SSHA process is concerned with the software portion of the system analysis.

3. The SRVT must also include recommended safety requirements that the PO declined to implement.

The SSHA process ensures that the system perspective is represented in the software development. As such, it must consider the safety impact of:

- Errors in algorithms, components, modules, routines, and calculations;
- Hazardous conditions (e.g., deadlocking, inappropriate magnitude, multiple event / wrong event environment, out-of-sequence / adverse environment, and inappropriate inputs or outputs);
- Software components whose performance, performance degradation, functional failure, or inadvertent functioning could result in a hazard, or whose design does not satisfy contractual safety requirements; and
- Software events, faults, and occurrences (such as improper timing).

The SSHA documents how the software performs its intended function safely. It does this by ensuring that the safety design criteria identified in the software requirement specifications have been satisfied and that the implementation choices have been evaluated so no unsafe conditions have been introduced.

4.2 Development Assurance Levels

Development Assurance Levels (DALs) are based on hazards identified during the SRM process. The choice of system design and architecture can invalidate current safety requirements and pose unanticipated hazards that could generate new safety requirements, potentially affecting the DAL. For example, architectural mitigation and partitioning techniques may be used to reduce the DAL. DALs from previous analyses should be revisited with the available design information. If DAL reduction is proposed, then the PO must be informed to ensure that the reduction can be evaluated and approved.

4.3 Commercial Off-the-Shelf Products

Using a Commercial Off-the-Shelf (COTS) product with a very high reliability as a sub-system or component of a sub-system will not automatically ensure a safe system, as reliability does not account for interactions with other system components. This is particularly important to remember with software because it usually controls many, if not all, of the interactions among system components. Simply equating software reliability or specification conformance with safety will not ensure an acceptable safety level of the system. There may be times when it is less expensive and safer to provide special-purpose software rather than a COTS product; using COTS products may amount to a false economy.

There are other times where COTS components may have adequate system safety. In these cases, the producer of that component must provide the prime contractor with either a complete “black box” behavior specification or an analysis that shows the component design allows protection against any possible hazardous software behavior. This information must be provided for a complete SSHA to be performed.

4.4 Tailoring

The PO must refer to an approved Program Safety Plan (PSP) to determine whether an SSHA must be conducted during a system acquisition. The PO may use methods other than an SSHA to capture required information or prepare a combined SSHA / System Hazard Analysis to meet FAA Acquisition Management System requirements only if such alternatives have been approved in the PSP.

SSHAs are usually developed for new systems; however, many acquisition programs deploy their capabilities incrementally over time and have an Initial Operating Capability date for each capability. In lieu of a new SSHA, additions to previously developed systems may require either updates to existing SSHAs, supplemental hazard analyses, or new hazard analyses. The specifics of such analyses must be defined in the approved PSP.

5 Use of the Analysis

An SSHA must:

1. Document sub-system compliance with requirements to eliminate hazards or reduce the associated risks.

    a. Validate applicable flow-down of design requirements from top-level specifications to detailed design specifications for the sub-system.

    b. Ensure that design criteria in the sub-system specifications have been satisfied and that verification and validation of sub-system mitigation measures have been included in test plans and procedures.

2. Identify previously unidentified safety hazards associated with the design of sub-systems.

    a. The implementation of sub-system design requirements and mitigation measures must not introduce any new safety hazards to the system. The PO must determine potential safety hazards resulting from modes of failure, including:

        - Component failure modes and human errors,
        - Single-point and common cause failures,
        - The effects when failures occur in sub-system components, and
        - The effects from functional relationships between components and equipment comprising each sub-system. Consider the potential contribution of sub-system hardware and software events, faults, and occurrences (such as improper timing).

3. Recommend necessary actions to eliminate previously unidentified hazards or mitigate their associated risks.

    a. Determine risk and the need for additional safety requirements to mitigate operational hazards. Develop system safety requirements to assist in preparing performance and design specifications.

    b. Ensure system-level hazards attributed to the sub-system are analyzed and that adequate mitigations are identified for possible implementation in the design as directed by the government.

4. Establish the framework for follow-up hazard analyses that may be required.

Appendix H
Conducting and Documenting a System Hazard Analysis

Conducting and Documenting a System Hazard Analysis

1 Background

1.1 Description

The System Hazard Analysis (SHA) is a safety analysis that the Program Office (PO) / system developer conducts to analyze system operation, system interactions, and system interfaces. It is initiated during the Solution Implementation phase and consolidates and builds upon the Sub-System Hazard Analysis (SSHA) and the Preliminary Hazard Analysis (PHA). The SHA identifies new hazards at system and sub-system interfaces and documents previously unidentified hazards. Ideally, the SHA identifies hazards and safety risks that were not identified in the SSHA as well as hazards and safety risks that apply to more than one sub-system.

The SHA, considering the system as a whole, analyzes the following areas that could contribute to system hazards:

- System operation
- Interfaces and interactions between:
    - Sub-systems
    - System and sub-systems
    - System and external systems
    - System and operators
- Component failures and normal (correct) behavior

Safety design requirements (some of which were generated during the PHA) that are included in the final Program Requirements Document are refined during the SHA; the system must be validated for conformance to these requirements. Through the SHA, safety design requirements are traced to individual components based on functional decomposition and allocation. As the system design matures, the SHA should be updated.

The Program Management Organization (AJM) must approve the SHA prior to the In-Service Decision review.

2 Process Overview

An SHA assesses the risks associated with the total system design (including software) by recognizing previously unidentified hazards associated with system interfaces, system functional faults, and system operation in the specified environment. It determines whether the method of implementing the hardware, software, facility design requirements, and corrective actions has impaired or degraded the safety of the system or introduced any new hazards. An SHA must also consider human factors, system/functional failures, and functional relationships between the sub-systems comprising the system (including software).

The methodology for conducting an SHA matches that of a PHA. The SHA follows the DIAAT process (**D**escribe the System, **I**dentify Hazards, **A**nalyze Risk, **A**ssess Risk, **T**reat Risk) identified in the Air Traffic Organization Safety Management System (SMS) Manual by identifying potential safety hazards, ranking them according to their severity and likelihood, and translating these potential hazards into high-level safety design requirements and hazard controls.

3 Preparing the SHA

Inputs into the SHA include:

- Design knowledge,
- Safety hazard knowledge,
- Output from the PHA,
- Output from the SSHA,
- Output from other analysis tools,
- Output of each phase of the formal software development process, and
- Test results.

3.1 Analysis Tools

In an SHA, a hazard causal analysis[1] is used to refine the high-level safety requirements into more detailed requirements. This process typically requires a model of the system. Causal analysis usually involves a search through the system design for system states[2] or conditions that could lead to system hazards.

Some examples of analysis tools that may contribute input to the SHA include:

- Fault tree analysis,
- Failure mode and effect analysis,
- Event tree analysis, and
- Interface analysis.

3.2 Reviewing and Approving the SHA

The PO must facilitate a peer review of the SHA and ensure that a copy is sent to the Safety and Technical Training (AJI) safety case lead for review and comment. The final document must be approved per AJM guidance. The PO must upload the SHA to the Safety Management Tracking System (SMTS) per the instructions in the SMTS User Manual.

3.3 Preparing/Revising the Safety Requirements Verification Table

The Safety Requirements Verification Table (SRVT) must contain all of the safety requirements identified (existing, validated, and recommended),[3] starting with the origin of the requirement, and must include those safety requirements identified in the SHA.

4 Other Considerations

The PO must refer to the approved Program Safety Plan (PSP) to determine which safety analyses/assessments must be conducted during a system acquisition. The PO may use methods other than an SHA to capture required information or may prepare a combined SSHA/ SHA to meet Federal Aviation Administration (FAA) Acquisition Management System requirements only if such alternatives have been approved in the PSP.

SHAs are developed for new systems; however, many acquisition programs deploy their capabilities incrementally over time and have an Initial Operating Capability date for each

1. In simple terms, a causal analysis is a process used to identify why something occurs. See the Federal Aviation Administration Systems Engineering Manual for further details.

2. Per the SMS Manual, a system state is the expression of the various conditions in which a system can exist. It is important to capture the system state that most exposes a hazard while remaining within the confines of any operational conditions and assumptions defined in existing documentation.

3. The SRVT should include recommended safety requirements that the PO declined to implement.

capability. In lieu of a new SHA, additions to these previously developed systems may require updates to existing SHAs, supplemental hazard analyses, or new hazard analyses. The specifics of such analyses must be detailed in the approved PSP.

Due to the complexity of the SHA, the analysis is usually identified in a procurement specification and conducted by the system developer. If so, the PO must include the need to conduct an SHA as a contractual requirement. An appropriate Data Item Description must be included as part of the contract. The PO must also require that Safety Risk Management (SRM) panels be conducted and that all SRM panels facilitated or conducted by the developer include subject matter experts, particularly those with an operational perspective. The FAA must actively review and be able to modify/comment on the safety analysis documentation as it is being prepared by the developer and not just at its final delivery. The developer must incorporate any valid comments received from the government's peer review process.

4.1 Development Assurance Levels

Development Assurance Levels from previous analyses should be revisited with the available design information.

4.2 Traceability to the PHA

If the SHA identifies a safety hazard that is new or cannot be traced back to one identified in the PHA, then the PO must update the PHA and submit it for approval by the Director of Policy and Performance, AJI-3.

5 Use of the Analysis

The SHA may be used to identify:

- Compliance with specified safety design criteria;
- Possible independent, dependent, and simultaneous hazardous events, including failures of safety devices, system failures, common cause failures and events, and system interactions that could create a hazard;
- Degradation in the safety of a sub-system or the total system from the normal operation of another sub-system;
- Design changes that affect sub-systems; and
- Effects of reasonable human errors.

An SHA recommends new/modified system requirements to eliminate identified hazards or to control their associated risks to acceptable levels, refines high-level safety design requirements, and provides a comprehensive analysis baseline for subsequent design changes.

Appendix I

Conducting and Documenting an Operating and Support Hazard Analysis

Conducting and Documenting an Operating and Support Hazard Analysis

1 Background

1.1 Description

The Operating and Support Hazard Analysis (O&SHA) is an important part of any System Safety Program. It is typically performed by the system developer in the later stages of Solution Implementation when system design details are known; it may be reviewed and updated as the system design matures to ensure that design modifications, procedures, and testing do not create new hazardous conditions.

The purpose of the O&SHA is to identify and evaluate the safety risk of National Airspace System (NAS) operations derived from the implementation of operating and support tasks. These tasks encompass procedures conducted by air traffic controllers as well as support functions conducted by aviation safety specialists. The O&SHA ensures that any safety risk in NAS operations resulting from interactions of the personnel performing system operation/support functions remains at an acceptable level. The O&SHA analyzes the safety risk of NAS operations by evaluating operating and support procedures, the system design, and the human-system integration interface. In addition, it proposes mitigations to the hazards identified from the analysis of these procedures and support functions.

The human (as both a receiver of inputs and an initiator of outputs during system operation) and human-system integration are essential elements of the total system. They are significant factors for consideration in the O&SHA as they create an effective link between human factors engineering analyses and system safety.

The O&SHA does not uncover design problems associated with hardware/software (as in the earlier safety risk analyses); rather, it identifies and evaluates the safety hazards associated with the operational environment, personnel, procedures, and equipment involved throughout the operation/support of a system as it impacts NAS operations.

The O&SHA identifies, documents, and evaluates safety hazards resulting from the implementation of operating and support tasks performed by personnel and considers:

- The planned system configuration at each phase of operation/support;
- The planned environments, support tools, or other equipment specified for use;
- The operation/support task sequence;
- Concurrent task effects and limitations; and
- The potential for unplanned events, including safety hazards, introduced by human error.

The Program Management Organization (AJM) must approve the O&SHA prior to the In-Service Decision.

2 Process Overview

The O&SHA analysis technique, which uses methodology similar to that of the Preliminary Hazard Analysis (PHA), identifies safety hazards presented in operating and support tasks as they impact NAS operations as well as the safety hazards' causal factors and effects. To ensure procedures focus on NAS operational safety (as opposed to safety impacts to the operators/maintainers), the change proponent must:

- Examine the procedure for effect, necessity, and clarity and consider that personnel may take shortcuts to avoid arduous, lengthy, uncomfortable, or ambiguous procedures;
- Examine each procedure and step—no matter how simple it appears—for possibilities of error, alternative actions, and adverse results;
- Determine whether special training, knowledge, or capabilities are required; and
- Review the potential causes of error and attempt to eliminate or minimize the possibility of occurrence.

2.1 O&SHA Goals

The goals of the O&SHA are to:

- Provide a system safety focus from a NAS operations perspective;
- Identify safety hazards related to tasks that may impact NAS operations and that are caused by factors such as design flaws, hardware failures, software errors, human errors, or poor timing;
- Propose system safety requirements to eliminate identified safety risk for NAS operations or reduce the associated risk to an acceptable level; and
- Ensure that all operating/support procedures maintain an acceptable level of safety risk in the NAS operational environment.

2.2 O&SHA Scope

The scope of the O&SHA includes the following operating/support events:[1] normal user operation, training, testing, assembly and installation, modification, maintenance and repair, support/monitoring/servicing, storage, handling, transportation, removal/disposal, emergency escape/rescue operations, and post-accident responses.

2.3 Preparing the O&SHA

2.3.1 Inputs

Prior to performing the O&SHA, appropriate task analyses should be conducted on all pertinent phases of operation/support. In addition, the following are some of the other possible inputs for an O&SHA:

- Previous safety analyses (e.g., PHAs, System Hazard Analyses, or Sub-System Hazard Analyses)
- Procedures
- Sequence diagrams
- Operation and functional analyses
- Equipment layout diagrams
- System and sub-system design specifications
- Equipment and interface drawings

1. Operating/Support events consist of sequenced actions that are generally documented in procedures.

- Operations and maintenance instructions
- Human factors engineering data
- Task design
- System/Operational design
- Hardware failure modes

2.3.2 Analyzing Procedures

An analysis of the operating/support procedures must be completed to ensure that:

- Required tasks, the human-machine environment, interpersonal interactions, and the sequence of operating/support steps will not create an unacceptable safety risk to NAS operations.
- Procedures do not expose personnel to any unacceptable safety hazards that may impact NAS operations.
- Instructions are clear and effective and do not introduce errors that could lead to unacceptable safety risk to NAS operations.
- Changes to software are conducted using a process at the same Development Assurance Level of the software, or as addressed via guidance in RTCA[2] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*, on:
    - Field-loadable software,
    - Option-selectable software,
    - User-modifiable software, and
    - Adaptation data.
- Alternative actions that could result in an aircraft accident or incident are precluded, or the effects of such actions are minimized.
- Safety-critical steps are highlighted with warnings and cautions, as necessary.
- No extraordinary mental or physical demands that could lead to unacceptable safety risk to NAS operations are required for programmed operations.
- Deadlines for the accomplishment of safety-critical tasks are realistic.
- Safeguards and detection/ warning devices operate as intended.
- Emergency stop systems can be reached and operate as intended.
- Personal protective equipment or devices can be reached and used within planned lengths of time.

2.3.3 Reviewing and Approving the O&SHA

The Program Office (PO) must facilitate peer review of the O&SHA and ensure that a copy is sent to the Safety and Technical Training (AJI) safety case lead for review and comment. The

2. RTCA, Inc., is a private, not-for-profit association founded in 1935 as the Radio Technical Commission for Aeronautics; it is now referred to simply as “RTCA.”

final document must be approved per AJM guidance. The PO must upload the O&SHA to the Safety Management Tracking System (SMTS) per the instructions in the SMTS User Manual.

2.3.4 Preparing/Revising the Safety Requirements Verification Table

The Safety Requirements Verification Table contains all of the safety requirements identified (starting with the origin of the requirement) and must include requirements proposed in the O&SHA.

3 Other Considerations

Due to the complexity of the O&SHA, the analysis is usually identified in a procurement specification and conducted by the system developer. If so, the change proponent (most likely the PO) must include the need to conduct an O&SHA as a contractual requirement. An appropriate Data Item Description (DID) must be included in the contract.

The PO must also require that a Safety Risk Management (SRM) panel be conducted and that all SRM panels facilitated or conducted by the developer include subject matter experts, particularly those with an operational perspective. The government must actively review and be able to modify/comment on the safety analysis documentation as it is being prepared by the developer and not just at its final delivery. The developer must incorporate any valid comments received from the government's peer review process.

Any proposed procedures must be verified through examination, demonstration, and testing. This verification should be done by testers not involved in writing the procedures. Additionally, a checklist should be used to assist in verifying the procedures, and testers should perform the procedures as prescribed and anticipate any alternative actions users might take.

3.1 Traceability to the PHA

If the O&SHA identifies a safety hazard that is new or cannot be traced back to one identified in the PHA, the PO must update the PHA and submit it for approval by the AJI-3 Director.

4 Uses of an O&SHA

An O&SHA provides:

- Corrective or preventive measures to minimize the possibility of an error resulting in an aviation incident or accident;
- Recommendations for changes in hardware, software, or procedures to achieve an acceptable level of safety risk in the NAS operational environment;
- Development of effectively placed warning and caution notes, as necessary;
- Requirements for special training information for personnel who will carry out the procedures; and
- Recommendations for special equipment, such as personal protective clothing or devices (e.g., antistatic wrist straps and mats), that may be required for tasks to be carried out without impacting the safety of NAS operations.

Appendix J
Documenting a System Safety Assessment Report

Documenting a System Safety Assessment Report

1 Background

1.1 Description

The System Safety Assessment Report (SSAR) confirms that appropriate system safety work was performed during system development prior to deployment into the National Airspace System (NAS) by:

- Describing or referring to the analyses, assessments, and tests previously performed during the design and development of the system to identify safety hazards inherent therein, and
- Discussing or referring to the results of analyses, assessments, and tests conducted to verify that safety criteria and requirements were verified.

1.2 Overview

The SSAR is a comprehensive evaluation of the safety risks assumed prior to the operational use of a developed system. It is crucial that the SSAR encompass all prior safety analyses for the given system. The SSAR provides management with an overall assessment of the safety risk associated with a system prior to its fielding; it is, in essence, the final pre-deployment safety "report card."[1] The SSAR documents all the safety features of the system design and discusses any previously identified procedural, operational, and hardware- or software-related safety hazards that may exist in the developed system, as well as the specific safety requirements implemented to reduce the risk of those hazards to an acceptable level.

For systems undergoing an Independent Operational Assessment (IOA), the SSAR must be updated to reflect IOA results, as appropriate. Safety findings documented during the IOA must be evaluated by the Program Office (PO) to determine whether further analysis is needed; appropriate mitigations and a monitoring plan must be developed for any safety hazards identified in the IOA. For small development programs or non-developmental item acquisitions for products with low safety risk hazards, the SSAR may be the only formal documentation of safety program activities / hazard assessment.

The Federal Aviation Administration (FAA) change proponent (most likely the PO) must develop the SSAR as a summary document. However, due to the complexity of the SSAR, the change proponent may identify the development of the SSAR as a requirement that must be included in the development/acquisition contract to be prepared by the system developer. If this is the case, the change proponent must include the need to prepare an SSAR as a contractual requirement. An appropriate Data Item Description (DID) must be included as part of the contract.

In most cases, the SSAR is the final Safety Risk Management (SRM) document required prior to operational use of a system (i.e., prior to declaring Initial Operating Capability (IOC)) or an In-Service Decision (ISD)). First-site IOC occurs when operational capability is declared ready for conditional or limited use by site personnel. This occurs after the capability is successfully installed and checked at the site and has undergone site acceptance testing and field familiarization processes. IOC requires satisfaction of operational requirements as well as full logistics support/training for technicians and air traffic controllers. Prior to the declaration of IOC or the ISD, the change proponent must:

1. The SSAR is a living document that may be updated as necessary even after initial system deployment.

- Submit the SSAR to Safety and Technical Training (AJI) for peer review, and
- Ensure that the document is signed and approved by Policy and Performance, AJI-3, per Air Traffic Organization Safety Management System (SMS) Manual requirements.

2 SSAR Input

The SSAR is a summary of all the safety analyses/assessments performed during system design/development and their findings, the tests conducted and their findings, and a compliance assessment. As a result, the SSAR must contain input from the sources below if performed or conducted.

- Testing
  - Development testing
  - Operational testing
  - Acceptance testing
  - Field familiarization
- IOA
- Operational Suitability Demonstration[2]
- SRM documents
  - Operational Safety Assessment
  - Comparative Safety Assessment
  - Preliminary Hazard Analysis (PHA)
  - Sub-System Hazard Analysis
  - System Hazard Analysis
  - Operating and Support Hazard Analysis
- System development assurance documentation (e.g., the Plan for Software Aspects of Approval, Software Accomplishment Summary, Plan for Hardware Aspects of Certification, Hardware Accomplishment Summary, and evidence of compliance)
- Post-Implementation Review (PIR)
- Other analyses, assessments, and tests

3 SSAR Organization

The SSAR must contain the elements described in Section 3.1 through 3.11 of this appendix.

3.1 Signature Page

The signature page includes the appropriate signature blocks for safety risk acceptance and SRM document approval. (See Section 6 of this appendix.)

2. Operational suitability testing evaluates the degree to which a product intended for field use satisfies its requirements in availability, compatibility, interoperability, reliability, maintainability, safety, and human factors. In addition, the testing validates the following requirement areas: logistics supportability, documentation, certification criteria, installation, operating procedures, and transition and training.

3.2 Executive Summary

The Executive Summary is a brief description of the scope of the safety assessment and its findings, including the total number of high- and medium-risk safety hazards, identified safety requirements, and any other significant issues identified. The Executive Summary must also contain the total number of safety requirements implemented.

3.3 System Description

This section is developed by referencing other program documentation, such as system specifications, requirement documents, technical manuals, the developer's System Safety Program Plan (SSPP), and system specifications. This section must include, or provide a reference that includes, the following information, as applicable:

- The purpose and intended use of the system
- A brief historical summary of system development
- A brief description of the system and its components, including the name, type, model number, and general physical characteristics of the overall system and its major sub-systems and components
- A brief description of the system's software and its role within the system
- A description of any other systems that are operated in combination with the system
- Photographs, charts, flow/functional diagrams, sketches, or schematics to support the system description, test, or operation

3.4 System Operations

Like the System Description section of the SSAR, the System Operations section is developed by referencing other program documentation such as technical manuals, the SSPP, and system specifications. This section must include the following information, as applicable:

- The procedures for operating, testing, and maintaining the system, including a discussion of the safety design features and controls incorporated into the system as they relate to the operating procedures
- Any special safety procedures needed to assure safe operation, testing, and maintenance, including emergency procedures
- Anticipated operating environments and any specific skills required for safe operation, testing, maintenance, transportation, or disposal
- Any special facility requirements or personal equipment to support the system

3.5 System Safety

This section must include a description of or reference to:

- The safety criteria and methodology used to classify and rank safety hazards,
- The analyses and tests performed to identify safety hazards inherent in the system, and
- Discussions of the management/engineering decisions affecting the residual risk at a system level.

3.6 Results of Analyses and Tests (and Other Verification Activities)

This section summarizes the results of the analyses performed and the tests conducted. It must contain a compliance assessment and sufficient evidence to demonstrate compliance with system development assurance requirements.

3.7 Hazard Identification

This is a narrative or tabular summary of the total number of safety hazards identified and a breakdown of the high-, medium-, and low-risk hazards. The summary must include a list of all hazards (by sub-system or major component level) that have been identified and considered since the inception of the program; and it must refer to the applicable sections of an SRM document or describe:

- The safety hazards identified, recommended safety requirements, and actions already taken to eliminate or control the identified hazards;
- How safety requirements associated with the identified hazards affect the probability of occurrence and the severity level of the potential accidents; and
- The residual risk that remains after the safety requirements are applied or for which no safety requirements could be applied.

This section must include a plot on the safety risk matrix (found in the SMS Manual) showing the residual risk based on the verification of the corresponding safety requirements.

3.8 Safety Requirements Verification Table

The Safety Requirements Verification Table (SRVT) is an evolving list of safety requirements that starts with a system's first safety assessment. It lists the safety requirements that have been verified and the status of requirements not yet verified (including information on when they will be verified). The PO must ensure all safety requirements are captured within the SRVT.

The SRVT must contain the following information:

- **Hazard identification:** This identifies each safety hazard.
- **Causes or contributing factors, combinations of which lead to the identified safety hazard:** This describes the origin of each hazard.
- **Safety risk evaluation:** This shows the results of the safety risk evaluation and indicates the initial and predicted residual risk (i.e., the risk that is present before and after the safety requirements are implemented).
- **Safety requirements:** This shows the safety requirements that form the basis for the reduction in risk between the initial and residual state of the system and may refer to another document that describes the controls in more detail.
- **Traceability data:** This shows traceability between controls / safety requirements, design requirements, and Verification and Validation (V&V) activities and includes:
    - **Requirement identification:** This points to the clauses in the design documentation that define requirements relating to a given risk control measure.
    - **Test identification:** This points to clauses in test procedures or other V&V documents that confirm the controls were implemented as agreed.

- **Method of safety requirement verification:** This describes the method used to verify safety requirements.
- **Status information:** This tracks the progress in completing SRM activities or highlighting incomplete activities and the plans for completing them.

3.9 Monitoring Plan

In the PHA, the PO establishes safety performance targets for all identified hazards and develops an operational monitoring plan to track these performance targets. The risk acceptor or his or her designee must conduct the monitoring for these targets. The plan for doing this must be summarized in the SSAR.

Also, the PO must recognize that:

- The SSAR may identify workarounds to safety requirements that were not implemented prior to initial deployment despite the ISD authority granting approval to deploy, and
- Additional safety requirements may be developed post-IOC as a result of an Operational Suitability Demonstration, IOA, or PIR.

If either of these conditions apply, the PO may need to develop additional or modified post-deployment monitoring plans as part of the SRM effort.

Refer to the SMS Manual or contact the AJI safety case lead for more information on safety performance targets and monitoring plans.

3.10 Conclusions and Recommendations

This section must include:

- A short assessment of the results of the safety program efforts;
- A statement—signed by the designated system safety representative (responsible for preparing the SSAR) and the appropriate FAA PO—confirming that all identified safety hazards have been eliminated or controlled to an acceptable risk level and the system is ready to proceed to deployment; and
- Recommendations applicable to the safe interface of the system in question with other systems.

3.11 SSAR References

This section is a list of all pertinent references such as test reports, preliminary operating manuals, and maintenance manuals used in compiling the SSAR.

4 Accomplishing the SSAR

The SSAR can be accomplished through one or more safety reviews. The types of safety reviews are listed below.

- **Periodic review:** These reviews are conducted throughout the life of the program. They evaluate the status of the hazards based on the verification of safety requirements and help in monitoring the safety requirements' effectiveness.
- **Phased review:** These reviews are conducted for defined portions of the implementation of solutions in the NAS. Phased reviews apply to a single Joint

Resources Council decision, which involves implementing a solution in steps or phases. As long as the implementation is incremental (i.e., performed in steps), each increment involves safety reviews to evaluate the status of hazards based on the verification of mitigating requirements for that particular phase.

- **Final implementation review:** These reviews are conducted for a program's ISD or IOC declaration.

5 Technology Refreshment Portfolio

For each sub–Acquisition Category (ACAT) 1 Technology Refreshment (TR) project within a TR portfolio, the portfolio Program Safety Plan (PSP) (or an approved project-specific PSP, if necessary) must specify what decision points will be held (most likely an ISD) before the product can be deployed to service delivery points. Before a sub-ACAT 1 TR project can be deployed, the AJI-3 Director must approve an SSAR. Most sub-ACAT 2 TR projects will not require an approved SSAR (unless otherwise specified in the portfolio's Execution Plan), as they are approved via the NAS Change Proposals / System Support Modification process.

6 Approving the SSAR

The SSAR must be reviewed in accordance with the AJI-facilitated peer review process and approved per the policy provided in the SMS Manual. The PO must upload the SSAR to the Safety Management Tracking System (SMTS) per the instructions found in the SMTS User Manual. The AJI-3 Director will not approve the SSAR if there is insufficient evidence of compliance with a system development assurance program.

Appendix K
Acronyms

Acronyms

AC	Advisory Circular
ACAT	Acquisition Category
AIR	Aircraft Certification Services
AJI	Safety and Technical Training
AJM	Program Management Organization
AJR	System Operations Services
AJT	Air Traffic Services
AJV	Mission Support Services
AJW	Technical Operations
AL	Assurance Level
AMS	Acquisition Management System
ANG	Office of NextGen
AOV	Air Traffic Safety Oversight Service
ARP	Aerospace Recommended Practice
ASOR	Allocation of Safety Objectives and Requirements
ASR	Airport Surveillance Radar
ATC	Air Traffic Control
ATM	Air Traffic Management
ATO	Air Traffic Organization
ATO-SG	Air Traffic Organization Safety Guidance
CC	Configuration Control
CCB	Configuration Control Board
CM	Configuration Management
CNS	Communication, Navigation, and Surveillance
ConOps	Concept of Operations
COTS	Commercial Off-the-Shelf
CRD	Concept and Requirements Definition
CRDR	Concept and Requirements Definition Readiness
CSA	Comparative Safety Assessment
DAL	Development Assurance Level
DID	Data Item Description
EA	Enterprise Architecture
EOC	Executable Object Code
EP	Execution Plan
EST	Enterprise Safety Team
FA	Functional Analysis
FAA	Federal Aviation Administration
FAST	FAA Acquisition System Toolset
FFBD	Functional Flow Block Diagram
FHA	Functional Hazard Assessment
FID	Final Investment Decision
FLS	Fire Life Safety
FM	Formal Methods

fPRD	Final Program Requirements Document
GSIP	Generic Site Implementation Plan
HAW	Hazard Analysis Worksheet
HEAT	Hazard Enterprise Architecture Traceability
IA	Investment Analysis
IAP	Investment Analysis Plan
IARD	Investment Analysis Readiness Decision
IID	Initial Investment Decision
IOA	Independent Operational Assessment
IOC	Initial Operating Capability
iPRD	Initial Program Requirements Document
ISD	In-Service Decision
ISM	In-Service Management
ISPD	Implementation Strategy and Planning Document
ISR	In-Service Review
ISSA	Integrated System Safety Assessment
JRC	Joint Resources Council
LOB	Line of Business
MB	Model-Based
NAS	National Airspace System
NextGen	Next Generation Air Transportation System
OHA	Operational Hazard Assessment
OI	Operational Improvement
OOT	Object-Oriented Techniques
ORM	Operational Risk Management
OSA	Operational Safety Assessment
OSED	Operational Services and Environment Description
OSH	Occupational Safety and Health
O&SHA	Operating and Support Hazard Analysis
OV-5	Operational Activity Model
PHA	Preliminary Hazard Analysis
PHAC	Plan for Hardware Aspects of Certification
PHL	Preliminary Hazard List
PIR	Post-Implementation Review
PMP	Program Management Plan
PO	Program Office
POC	Point of Contact
PR	Problem Report
PRD	Program Requirements Document
pPRD	Preliminary Program Requirements Document

PSAA	Plan for Software Aspects of Approval
PSP	Program Safety Plan
PST	Program Safety Team
RBDM	Risk-Based Decision Making
SAS	Software Accomplishment Summary
SCI	Software Configuration Index
SCL	Safety Case Lead
SCMP	Software Configuration Management Plan
SCT	Safety Collaboration Team
SDLC	Software Development Lifecycle
SDP	Software Development Plan
SECI	Software Environment Configuration Index
SEM	Systems Engineering Manual
SHA	System Hazard Analysis
SI	Solution Implementation
SLSA	Service Level Safety Assessment
SME	Subject Matter Expert
SMS	Safety Management System
SMTS	Safety Management Tracking System
SOC	Safety Oversight Circular
SOW	Statement of Work
SPP	Safety Program Plan
SQA	Software Quality Assurance
SQAP	Software Quality Assurance Plan
SRM	Safety Risk Management
SRMGSA	Safety Risk Management Guidance for System Acquisitions
SRVT	Safety Requirements Verification Table
SSAR	System Safety Assessment Report
SSHA	Sub-System Hazard Analysis
SSM	Safety Strategy Meeting
SSP	System Safety Program
SSPP	System Safety Program Plan
SSW	Safety Strategy Worksheet
SU	Service Unit
SV-4	Systems Functionality Description
SVP	Software Verification Plan
T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TQ	Tool Qualification
TQL	Tool Qualification Level
TR	Technology Refreshment
V&V	Verification and Validation