To All Users:

The Safety Risk Management Guidance for System Acquisitions (SRMGSA) version 2.0 will be effective on September 1, 2014. Continue to adhere to SRMGSA version 1.5 through August 31, 2014. For inquiries, contact Safety and Technical Training at 9-AJI-SMS@faa.gov.

Air Traffic Organization
Safety and Technical Training

SRMGSA

Safety Risk Management Guidance for System Acquisitions Version 2.0

Air Traffic Organization 2014

ALL POINTS/SAFETY
everyone. everywhere. everyday.

FAA
Air Traffic Organization

Table of Contents

Appendices

Preface

This version of the Safety Risk Management Guidance for System Acquisitions (SRMGSA) cancels SRMGSA Version 1.5. It applies to acquisitions that have an effect on the National Airspace System (NAS) when the acquired systems are fielded. The SRMGSA has been expanded to include new information pertaining to the Federal Aviation Administration (FAA) Acquisition Management System (AMS) changes, Next Generation Air Transportation System (NextGen) Portfolio Management, and integrated safety management. In addition, the SRMGSA has been restructured. 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 is contained in the appendices to the SRMGSA.

The SRMGSA is the required guide for applying SRM to acquisitions that affect the NAS. ATO Safety and Technical Training (AJI) is the focal point for determining what in acquisitions affects NAS safety. AJI is the Office of Primary Responsibility for the SRMGSA.

1 Introduction

The SRMGSA defines the scope, purpose, objectives, and required activities of the FAA's systems safety effort as it applies to SRM for all system acquisitions that provide Communication, Navigation, and Surveillance (CNS), Air Traffic Management (ATM), and other services in the NAS.[1] The SRMGSA applies to all personnel in the ATO performing safety risk assessments and is of interest to those performing a similar role for the Assistant Administrator of the Office of NextGen (ANG), the Office of Airports (ARP), or other FAA Lines of Business (LOBs).

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
- The fostering of personal accountability and corporate self-regulation in safety matters.

Order 1100.161, *Air Traffic Safety Oversight*, identifies the acquisition and implementation of new systems as a focus of the Air Traffic Safety Oversight Service's (AOV's) oversight efforts. Per AOV Safety Oversight Circular (SOC) 09-11, *Safety Oversight*, new acquisitions are required to follow the guidance of the FAA AMS and meet the program requirements defined in the ATO Safety Management System (SMS) Manual and the SRMGSA.

1.1 Purpose

The purpose of the SRMGSA is to meet the requirements of and implement the policy stated in section 4.12 of the AMS. Section 4.12 requires the application of an SMS, referring to the ATO SMS Manual and the SRMGSA as the guidelines to follow. Thus, the SRMGSA provides the

[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 https://nasea.faa.gov/requirements/enterprise.

guidelines to be used by the ATO and other organizations when conducting SRM in acquisitions. The purpose of SRM is to maintain or improve the safety of the NAS by identifying, managing, and mitigating the safety risk associated with making changes to the NAS.

The primary goal of the SRM process is the development and incorporation of safety requirements. When system[2] hazards are identified, the subsequent mitigations that are derived from the SRM process (as described in the ATO SMS Manual) are translated into requirements for the acquired systems. In order to achieve the residual risk predicted in the SRM process, it is crucial that the requirements be connected to the Verification and Validation processes. Without these connections, safety performance and the true residual risk cannot be determined.

The SRMGSA provides a framework and further process definition to ensure the execution of SRM throughout the entire lifecycle of a system or product. This framework is made formal in the Program Safety Plan (PSP) developed for a program by a Program Safety Team (PST). (Refer to appendix A for guidance on developing and implementing PSPs and section 4.7 for more information on PSTs.) The SRMGSA follows systems engineering principles to achieve SRM objectives defined in the various FAA/ATO orders listed in section 3.

The SRMGSA defines the ATO's processes for ensuring that systems safety[3] is effectively integrated into system changes and NAS modernization in accordance with FAA orders, the ATO SMS Manual, and AMS policy.[4] It describes the AMS phases, organizational roles and responsibilities, program requirements, tasks, and reporting requirements associated with performing SRM within the ATO and other organizations involved in acquisitions that affect the NAS (e.g., Office of Aviation Safety (AVS), ARP, and ANG).

The SRMGSA provides the following:

- Safety management guidance for acquisitions during the following phases of the AMS lifecycle:
  - Service Analysis and Strategic Planning
  - Concept and Requirements Definition (CRD)
  - Investment Analysis (IA)
  - Solution Implementation
  - In-Service Management (ISM)

[2] A "system" is a set of interacting or interdependent components forming an integrated whole. A system is characterized by:

- Structure: It contains parts (or components) that are directly or indirectly related to each other.
- Behavior: It contains processes that transform inputs into outputs (material, energy, or data).
- Interconnectivity: The parts and processes are connected by structural and/or behavioral relationships.

A system's structure and behavior may be decomposed via sub-systems and sub-processes to elementary parts and process steps.

[3] Systems safety is an integrated set of constituent pieces that are combined in an operational or support environment to accomplish a defined objective. These pieces include people, equipment, information, procedures, facilities, support, and other services. The term "safety" includes any technical, social, educational, and/or managerial action initiated to eliminate or reduce the hazards associated with a procedure or system (e.g., risk of property loss and personal injury).

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

- Specific guidance for system changes
- A definition of the Joint Resources Council's (JRC's) expectations regarding SRM

The SRMGSA describes the organization and responsibilities of FAA management, the ATO, and ANG for fulfilling SRM objectives. It also addresses AJI's relationship within the ATO (specifically with the Program Management Organization (PMO) and the Service Units) and with ANG for developing and approving safety documentation and accepting risk prior to JRC decisions.

The SRMGSA is supplemented by the following ATO-SGs:

- ATO-SG-14-01, *Development Assurance for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*
- ATO-SG-14-02, *Software Assurance Approval Guidelines for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*
- ATO-SG-14-03, *Conducting a DO-278A Software Assurance Compliance Gap Analysis for Acquired NAS Systems*

When a change affects the accepted scope of performance or requirements, the SRMGSA may be revised upon agreement between AJI, the ATO PMO, the ATO Chief Safety Engineer, and the Acquisition Systems Advisory Group. The AJI Integrated Safety Policy Team is responsible for revising and maintaining the SRMGSA.

1.2 Scope

The SRMGSA supports the goals of the AMS process with guidance focused on service delivery and an improved transition of programs from research and development to implementation.[5] AMS policy, FAA/ATO orders, and the ATO SMS Manual mandate a planned and organized SRM approach to decision-making 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 between ATO organizations, ANG, and other LOBs. This 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 systems 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 ATO SMS Manual before they can be fielded. This includes leased services / vendor-provided services that affect the safety of the NAS.

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

2 Safety Management Policy

2.1 Acquisition Management

AMS section 4.12 in the FAA Acquisition System Toolset (FAST) contains the AMS policies for the safety management of NAS acquisitions. This section requires that:

- Safety management be conducted and documented throughout the lifecycle of a system,
- SRM be used to identify safety risks in the NAS, and
- Product development be conducted at a rigor commensurate with the severity of the hazard that would result from a failure of the product.

2.2 Systems Safety

The Program Manager (PM) must institute a systems safety program that meets the requirements of the ATO SMS. The status of systems safety must be presented at all decision points and investment reviews. Detailed guidelines for safety management and development assurance are found in the FAST; the ATO SMS Manual; RTCA DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*;[6] and the ATO-SGs[7] referenced in this document.

2.3 Integrated Safety Management

The highly distributed and interconnected nature of NextGen presents complex safety challenges to the NAS. In addition, many changes to the NAS necessary to implement NextGen initiatives may occur in a parallel or overlapping manner. The past SRM paradigm was focused on analyzing individual changes; it was insufficient for addressing all the hazards identified as a result of planned NextGen interactions and interconnectivity.

The legacy NAS is a “System of Systems,” providing multiple services to users. With NextGen, the NAS is evolving into an even more complex configuration. Future acquisitions are beginning to blur the lines of 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 build on one another, subsume each other, or combine for a joint function or capability. This perspective was not considered historically, but will be important to applying the concept of integrated safety in acquisitions.

Integrated safety management represents a more robust, holistic, and integrated approach to performing safety analysis. Integrated safety management uses existing safety policy and methodologies, as well as systems engineering processes. Integrated safety management is a critical component not only for successfully achieving the NextGen vision, but for all enhancements to the NAS. Safety assessments using integrated safety management principles must be conducted in three “directions”: vertical, horizontal, and temporal.

Vertical integration ensures the consistency of safety assessments across hierarchical levels, from the program or system level up to the NAS level. Horizontal integration ensures that the interactions and interdependencies across organizations, operational capabilities, NextGen

[6] An RTCA user identification and password are required to down load RTCA documents. FAA employees may obtain an RTCA membership username and password by contacting RTCA.

[7] See the current version of Order JO 1030.1, *Air Traffic Organization Safety Guidance*, for information concerning the ATO-SG program.

Portfolios,[8] Operational Improvements (OIs),[9] increments,[10] and individual programs or systems are addressed in safety assessments. Temporal integration ensures that the impacts of hazards and their associated mitigations across implementation timelines are understood and considered. This reflects and accounts for the significant amount of time and development effort it takes to implement NextGen initiatives, many of which interact but are not scheduled to enter service at the same time.

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 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.

2.4 Software-Intense Systems

Software-intense systems must demonstrate that a software product was developed at an appropriate level of rigor. The establishment of a development assurance program in accordance with RTCA DO-278A is one acceptable means[11] of demonstrating this level of rigor.[12] See section 6.3 for additional details.

3 References

The current versions of the following FAA orders and guidance documents supplement the SRMGSA:

- The ATO SMS Manual
- The FAA AMS Policy / FAST
- The FAA System Safety Handbook
- Order JO 1000.37, *Air Traffic Organization Safety Management System*
- Order 8040.4, *Safety Risk Management*
- Order 1100.161, *Air Traffic Safety Oversight*
- Order 6032.1, *National Airspace System (NAS) Modification Program*
- Order JO 1030.1, *Air Traffic Organization Safety Guidance*
- Order JO 6000.50, *National Airspace System (NAS) Integrated Risk Management*
- AOV SOC 09-11, *Safety Oversight*
- 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, *AOV Guidance on Safety Risk Modeling of High-Risk Hazards*

[8] A NextGen Portfolio is defined as a set of capabilities that share a common benefits pool within a common operational space. ANG administers or manages the NextGen Portfolios.

[9] An OI is a distinct strategic activity for service delivery to improve NAS operations and move toward a NextGen vision.

[10] An increment is a portion of an OI that will deliver an incremental benefit.

[11] Subject to approval by the ATO Chief Safety Engineer, a developer's internal procedures may also suffice.

[12] The software development assurance process is covered by ATO-SG-14-02, *Software Assurance Approval Guidelines for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*.

- RTCA DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*

4 Roles and Responsibilities

The organizational roles and objectives involved in the AMS SMS are designed to ensure that the following objectives are met:

- Systems under consideration for inclusion in the NAS are evaluated systematically (i.e., from vertical, horizontal, and temporal perspectives) and at an appropriate time to assist in decision-making.
- 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.
- Hazards are identified, assessed for risk, and 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 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.
- Integrated Safety Risk Management (ISRM) is conducted within each portfolio to provide a complete picture of the potential safety risk of fielding a particular NextGen capability (see section 4.2). Appendix B gives detailed guidance concerning ISRM.

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

The roles and responsibilities of each organization involved in implementing the AMS and ISRM in system acquisitions are detailed below. A complete description of roles and responsibilities for the JRC and organizational entities can be found on the FAST website at http://fast.faa.gov/.

4.1 JRC Secretariat

The JRC Secretariat maintains the AMS-based JRC Readiness Criteria Checklist, which ensures that the appropriate SRM documents required for all investment decision meetings have been coordinated with AJI. The ATO Chief Safety Engineer will determine the completion of SRM documentation (either a Safety Risk Management Document (SRMD) or a Safety Risk Management Decision Memorandum (SRMDM)) for programs progressing through the FAA AMS and advise the JRC Secretariat as to his or her decision.[13]

4.2 Assistant Administrator for ANG and NextGen Portfolio Management

Within a NextGen Portfolio, there will be OIs, Operational Sustainments (OSs),[14] increments, and procedure and documentation changes, all of which must work together to deliver the

[13] The SRM documentation is not forwarded to the JRC Secretariat for review. The Secretariat only requires a notification from the ATO Chief Safety Engineer that the program has met its SRM obligations, as required by the AMS.

[14] An OS is an activity to sustain NAS services. (In these cases, an OI may have already been fielded.)

required capabilities. To provide a complete picture of the potential safety risk of fielding a particular capability (e.g., an OI), it is essential to conduct ISRM across that capability. The ANG NextGen Investment Portfolio Leads are responsible for all aspects of their portfolio, including ensuring the conduct of ISRM.

Some portfolios may have more than one FAA organization responsible for implementing their capabilities. ANG will interface with the operational Service Units (e.g., ATO Air Traffic Services (AJT) and ATO System Operations Services (AJR)) through the ATO PMO as much as practical. ATO Mission Support Services (AJV) will support NextGen Portfolios during the CRD phase and will bring together AJR/AJT inputs. The ATO PMO will provide support during the IA and Solution Implementation phases, and ATO Technical Operations Services (AJW) will provide support during the ISM phase.

In general, the SRM work at the solution, procedure, and document change levels will be conducted by the ATO PMO, AJV, and AJW following the SRM process described in the ATO SMS Manual. However, at the capability level, the ANG NextGen Investment Portfolio Leads have the responsibility for ensuring the conduct of safety assessments. The Portfolio Leads will typically seek the assistance of the ANG Office of Engineering Services, the ATO PMO, and AJI in conducting these assessments. In the conduct of ISRM, it is particularly important to properly set the scope of the safety assessments, as there are numerous complex relationships among systems, procedures, OIs, and OSs. The scope of a safety risk assessment at this level must be broad enough to include all potentially interacting functions, procedures, and airspace and system components.

To develop safety assessments with these broader scopes, the ANG NextGen Investment Portfolio Leads must:

- Ensure that capabilities under consideration are analyzed early (i.e., prior to the Investment Analysis Readiness Decision (IARD) phase) for possible safety ramifications due to integration with other NAS components.
- Identify how the magnitude of the safety issues/concerns identified early in capability development may impact the way the capability is considered for further investment and development.
- Support the transition of the capability to an implementing organization within the ATO, resulting in an SMS-compliant Operational Safety Assessment (OSA) prior to the IARD.
- Gather data on, understand, and articulate the safety issues/concerns as a capability evolves and moves through the acquisition lifecycle.

These assessments will be documented in Capability Safety Assessment (CapSA) Reports.[15] A Capability Safety Team (CST) chartered by the Portfolio Manager (see section 4.4) will perform the ISRM to produce the CapSA Report and support the safety efforts of the capability as it moves through the acquisition lifecycle.

4.3 Office of Aviation Safety

AVS includes AOV, which oversees the SRM process for system-oriented safety standards related to the acquisition and implementation of new systems in accordance with the current

[15] See appendix B for further guidance.

versions of Order 1100.161 and AOV SOC 09-11.[16] AVS roles and responsibilities are further defined in the NextGen Segment Implementation Plan.[17] It is important to note that AOV must approve any mitigations identified in an SRMD that lower the safety risk of any initially identified high-risk hazard before those mitigations may be implemented and the system(s) may be fielded.

4.4 Capability Safety Team

A CST is a resource to support the safety efforts of the ANG Portfolio Manager. The CST will help perform the ISRM to produce a CapSA Report and other required safety work (e.g., safety input into the Operational Capability Integration Plan). The CST will consist of stakeholders relevant to the capability regardless of organizational affiliation. The PMO, ANG, and AJI will always be CST members. Other CST members will depend on the OIs/OSs being considered. CST membership may change depending on the acquisition phase. The AJI representative on the CST will be an AJI Safety Case Lead, who will remain with the capability throughout its lifecycle. An AJI Safety Case Lead is an AJI safety engineer well-versed in systems safety, NAS operations, the Enterprise Architecture (EA), and engineering principles.

ANG and AJI will approve the CapSA Report. The AJI approver will be the ATO Chief Safety Engineer. The ANG approver will be the ANG Safety Manager. The ANG Advanced Concepts & Technology Development Office and the ATO Operational Concepts, Validation, and Requirements Directorate will break down and allocate capability requirements (including safety requirements) to individual programs/projects. The ATO PMO will manage these programs/projects. Some members of the CST will become members of the PSTs, which will support the individual programs (see section 4.7). The AJI Safety Case Lead will remain with these programs/projects and support the individual PSTs when they are formed.

4.5 Safety Collaboration Team

The NAS Safety Collaboration Team (SCT) is a group of safety stakeholders across LOBs facilitated by ANG to encourage collaboration and raise awareness of integrated safety issues. The SCT supports the development and advancement of ISRM and enhances risk-based decision making for NAS system acquisitions. The SCT may provide information and advice to the CST.

4.6 Integrated Safety Team

The Integrated Safety Team (IST) is appointed by the SCT to conduct ISRM and produce Integrated System Safety Assessments (ISSA) Reports. Performing ISRM to produce an ISSA Report differs from using the process to produce a CapSA Report in that its scope is not fixed around a capability. Its purpose is to identify the safety issues that may eventually be categorized as hazards early in the lifecycle, and to identify unmanaged risks in safety analyses by assessing across the three planes. The ISSA Report will provide safety/risk information to SRM processes such as CapSA- and program-level safety assessments. Unlike a CapSA, the ISSA might only be performed once and therefore, not be iteratively updated.

The IST will be composed of select representatives from the SCT with specific knowledge or expertise in the subject area of safety that is under consideration. As a sub-team of the SCT, the IST will have access to safety professionals from all stakeholder LOBs to foster the integrated safety management approach. The IST will begin performing ISRM early in a

[16] This SOC provides systems-oriented information and guidance material that may be used by the ATO to develop and implement procedures to comply with Order 1100.161.

[17] The NextGen Segment Implementation Plan is the FAA's blueprint for achieving the mid-term OIs.

concept's lifecycle. The IST is responsible for:

- Thoroughly conducting ISRM,
- Developing a detailed ISSA Report,
- Revising the ISSA Report as the concept matures and/or the ISSA safety issues are integrated into program safety documents,
- Presenting ISSA Report recommendations to the SCT, and
- Participating in AJI's safety case peer review process to ensure the alignment of program-level SRMDs with CapSA Report / ISSA Report recommendations.

4.7 Program Safety Team

A PST is a resource provided by the program to support the safety efforts of the acquisition throughout the AMS lifecycle. The PST may consist of a single safety Point of Contact (POC) or a team of safety experts, depending on the size and complexity of the program.

The PST, in conjunction with the AJI Safety Case Lead, 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 POC to coordinate all safety analyses throughout the program's lifecycle.
- Participate in the Safety Strategy Meetings (SSMs), as needed, 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 FAST, the ATO SMS Manual, ATO-SGs, and this document.
- Submit the proposed PSP and completed SRMDs or SRMDMs to the AJI Safety Case Lead for review and coordination to ensure timely decisions in support of JRC milestone decisions.
- Enter safety tracking and monitoring data into a safety management tracking system provided by AJI.
- Ensure that safety assessment and analysis results are addressed in program planning and requirements documents.
- Ensure that any requirements developed as a result of the safety analyses are included as discrete requirements in the preliminary Program Requirements Document (pPRD), the initial Program Requirements Document, or the final Program Requirements Document
- Ensure that the safety requirements are traceable back to identified safety hazards.
- Verify that the mitigations identified to reduce hazard risk are developed in accordance with the SMS and are included as validated and verified safety requirements in the final SRMD.
- Maintain safety documentation throughout the system lifecycle.

4.8 Air Traffic Organization

4.8.1 Roles and Responsibilities

Depending on the acquisition phase of the program, the ATO PMO, AJV, or AJW will have the responsibility of ensuring that ISRM has been conducted and the necessary documentation has been prepared at the increment level. They will be supported as appropriate by Subject Matter Experts (SMEs) from AJR, AJT, and/or AJW. Safety professionals within AJI will also support the CSTs/PSTs in preparing the safety documents and representing their functional discipline at reviews with the ATO Chief Safety Engineer. AJI and the Service Unit representatives to the CSTs/PSTs will ensure that the vice presidents of the involved Service Units are informed of the risks involved in a proposed change to the NAS and will recommend that they approve SRM documentation and accept risk, as necessary, in accordance with the ATO SMS Manual.

Specifically, AJV's role is to break down the FAA's Concept of Operations into operational needs. These operational needs will then be aligned with new/existing OIs or OSs 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.

The NAS EA[18] contains roadmaps that describe the transition from the "as is" to the "to be" environment. It aligns the FAA's mission, benefits, and capabilities in relation to its investments. Within the ATO, the ATO PMO coordinates the EA support effort for all roadmaps (except the safety roadmap) by providing the alignment of systems and technologies with the mission/business leads. This includes ensuring the application of the SMS in all ATO-managed acquisition programs.

AJI is the ATO's focal point for safety and provides the ATO with safety direction while driving the SRM/ISRM process. AJI coordinates the EA support efforts of the safety roadmap for the ATO.

Figure 4.1 summarizes the ATO's safety roles and responsibilities. Refer to table 9.1 to see which organization is typically responsible for the various safety analyses that will be conducted.

[18] Go to https://nasea.faa.gov for more information concerning the EA.

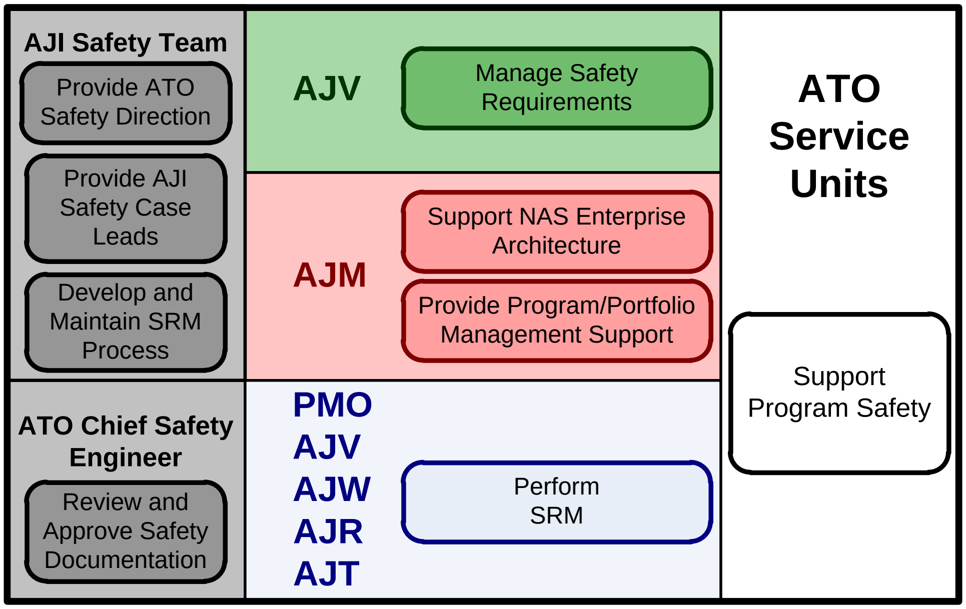

AJI Safety Team
Provide ATO Safety Direction
Provide AJI Safety Case Leads
Develop and Maintain SRM Process
ATO Chief Safety Engineer
Review and Approve Safety Documentation
AJV
Manage Safety Requirements
AJM
Support NAS Enterprise Architecture
Provide Program/Portfolio Management Support
PMO
AJV
AJW
AJR
AJT
Perform SRM
ATO Service Units
Support Program Safety

Figure 4.1: ATO Roles and Responsibilities

4.8.2 ATO Chief Safety Engineer

The primary function of the ATO Chief Safety Engineer is to provide 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.

The ATO Chief Safety Engineer must:

- Represent the ATO in resolving high-level safety issues in air traffic operation and decision-making meetings.
- Review and approve SRM documentation associated with NAS changes that require AOV approval, as defined in Order 1100.161.
- Review and approve SRM documentation for acquisition programs and safety assessments for changes done at the national level, as defined in the ATO SMS Manual and the SRMGSA.
- Review and approve safety input in support of JRC decisions, as required.
- Review and approve safety input to the NextGen Management Board (NMB) through the NextGen Portfolio Managers.
- Serve as the AJI focal point for collaboration with the ANG and the PMO on NextGen transitional activities with regard to safety.
- Collaborate with the ANG Safety Manager in the development of the CapSA Report and review its findings before presentation to the NMB.

- Advocate membership of an AJI Safety Case Lead on each capture team to ensure safety requirements are appropriately allocated in planning activities.
- Continuously reassess the original CapSA Report presented to the NMB to ensure that safety findings are representative of actual safety concerns and safety risks involved as the portfolio matures.
- Ensure that the safety case management process includes ISRM for a comprehensive safety review of concepts, solutions, systems, and procedures.
- Provide the Director for Policy and Performance and the Vice President of AJI with senior-level input on ATO safety-related issues for air traffic operations, acquisitions, and second level engineering.
- Review and approve safety input to the NAS EA safety roadmap and National Aviation Research Plan.
- Review and approve proposed changes to safety policy and guidance for incorporation in Order JO 1000.37, the ATO SMS Manual, and the SRMGSA.
- Collaborate with internal and external stakeholders to facilitate resolution of safety decisions that cross LOBs.
- Approve RTCA DO-278A (or equivalent document) lifecycle data.

4.8.3 AJI Safety Case Leads

The AJI Safety Case Leads are experts in SMS policy and guidance that pertain to the AMS. The AJI Safety Case Leads assist the CSTs/PSTs responsible for conducting or managing systems safety programs. For operational/new capabilities, AJI Safety Case Leads support the CSTs. For acquisitions, they assist the PST with conducting or managing systems safety programs.

The AJI Safety Case Leads are the ATO’s acquisition safety focal point, and ensure that each safety product associated with an AMS milestone is peer reviewed, and that all resulting comments and concerns are addressed prior to the program’s successful milestone decision. The AJI Safety Case Leads must:

- Meet with the CSTs/PSTs and conduct SSMs, as needed, to ensure timely development of SRM documentation in support of JRC milestones, starting in the CRD phase and ending during the ISM phase.
- Work with a CST/PST when assigned by the AJI Safety Engineering Team Manager and guide the CST/PST in conducting and developing the safety analysis and the PSP. As the SRM documentation is being developed, the AJI Safety Case Leads provide periodic feedback to the CST/PST. At the appropriate time, they recommend to the AJI Safety Engineering Team Manager that the SRM documentation is ready to enter the peer review process for approval and signatures.
- Coordinate the peer review (see section 8.3) of SRM documentation within a time that is consistent with the planned JRC decisions. This review must, at a minimum, ensure that the cause and effect relationship between proposed changes to the NAS and the risks to the operational safety of the NAS are explicitly analyzed and documented.
- Serve on capture teams representing the entire ATO from a safety perspective.
- Co-lead CSTs with the ANG NAS Systems Engineering Services Office, as requested.

- Identify, evaluate, and document lessons learned.

4.8.4 Program Manager

There are many functions performed by a successful PM that are beyond the scope of the SMS and this document. 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 includes ensuring that SMS is part of the decision-making process. Whether SRM is a collateral duty of one person or performed by a dedicated safety team, the PM ensures that SMS policy and guidelines are followed.

When assigning a safety lead or a safety team, the program or project manager should choose people who are able to:

- Communicate with program stakeholders,
- Understand program objectives,
- Understand program plans and acquisition strategy,
- Develop strategy 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 activity.

4.8.5 AJI Safety Engineering Team Manager

For new SRM efforts related to acquisitions and capabilities, the AJI Safety Engineering Team Manager is the first AJI POC for program and portfolio managers. The Safety Engineering Team Manager manages the safety case work load for a team of safety engineers and assigns an AJI Safety Case Lead to work with an individual program or capability portfolio based on resource availability. The Safety Engineering Team Manager ensures that SRM documentation and RTCA DO-278A or related lifecycle data is processed in accordance with the ATO SMS Manual, relevant ATO-SGs, and the SRMGSA before being submitted to the ATO Chief Safety Engineer for approval and signature.

The AJI Safety Engineering Team Manager must:

- Assign an AJI Safety Case Lead to work with a PST or CST.
- Balance the work load among AJI Safety Case Leads, considering commonality with existing assignments, their experience and expertise, and program and portfolio complexities.
- Confirm that any documentation being submitted to the ATO Chief Safety Engineer for approval has, at a minimum, been developed and peer reviewed in accordance with the SRMGSA and internal AJI processes.

4.8.6 Independent Safety Assessment Team

The AJI Independent Safety Assessment (ISA) Team is responsible for evaluating designated acquisition systems (and major modifications) through the Independent Operational Assessment (IOA) function. To ensure that solutions are within acceptable levels of safety risk, the ATO SMS and the AMS require that IOAs be conducted on designated systems prior to the In-Service Decision (ISD) to identify safety hazards and operational concerns in a representative operational environment. During the ISM phase, the ISA Team 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. More detailed information on IOAs may be found in the FAST.

5 Safety Planning for Acquisitions

5.1 Portfolio Safety Strategy

As described in section 4.2, the ANG NextGen Investment Portfolio Leads are responsible for ensuring the conduct of ISRM within their portfolio. This is not an independent effort; ANG needs to rely on the input of AJI to fully assess the safety posture of any portfolio and to plan ISRM efforts. At a high level, AJI will support ANG and NextGen ISRM by providing safety program information input to NextGen planning documents, such as the NextGen Implementation Plan and the NextGen Segment Implementation Plan. AJI will also provide consolidated ATO safety review of these NextGen planning documents. AJI support also includes:

- Forming an ATO safety perspective and managing the entire ATO capture process, including all aspects of the NextGen integrated safety management program;
- Collaborating with ATO stakeholders to ensure that safety artifacts are developed as needed during the capture process;[19]
- Developing a single ATO safety strategic plan to support NextGen concepts and implementation as depicted on the NAS EA safety roadmap, as well as tracking ATO Safety Decision Points on the EA safety roadmap;
- Approving the scope of NextGen safety assessments during the capture process in the pre-investment phase;
- Reviewing and approving SRMDs for the NextGen solutions; and
- Reviewing and approving safety OIs' functionality and implementation dates in the NextGen Safety Portfolio.

In addition, AJI and the PMO will work with the ANG NextGen Investment Portfolio Leads to identify any ISRM gaps that may exist within a portfolio. AJI will attend NextGen Portfolio Management reviews to identify and respond to NextGen-generated safety issues and documentation.

5.2 Safety Strategy Meetings

Acquisition strategies vary among investment programs. As a result, the SRM documentation requirements will also vary. The PMO/PST should contact AJI to schedule an SSM to

[19] The ANG thrust will be prior to the CRD and the IA phases of the process.

determine the appropriate documentation requirements and for guidance in fulfilling their SRM obligations for the AMS milestone being sought. The AJI Safety Case Lead will facilitate the SSM, contributing their knowledge of policies and SRM practices and ensuring that the proceedings are captured in the minutes. The SSM should be conducted in consultation with the ATO Chief Safety Engineer, if necessary, and particularly if extensive documentation tailoring is planned.

The SSM can be held at any time per the request of the program office. However, in order to gain the maximum benefit to the program, the SSM should occur early enough in the process to schedule SRM documentation development, review, coordination, and necessary approvals prior to the investment milestone decision point. SRM is a required checklist item for the IARD, Initial Investment Decision, Final Investment Decision, and ISD.

In addition to the overall safety strategy, the PSP and any other SRM products (OSA, Comparative Safety Assessment, etc.) may be discussed. Guidance in their development can be provided upon request. Meeting minutes containing the strategy agreed upon for satisfying acquisition SRM requirements are produced for each SSM.

The ANG Safety and Information Security Services Division will be an invited participant in all SSMs. For SSMs held for programs in or about to enter the CRD phase, the PMs must consult with the ANG CRD lead before the SSM convenes.

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 can be scheduled as often as is necessary.

6 Other Considerations

6.1 Baseline Change Management

For any acquisition program under its jurisdiction, the JRC approves and baselines all required AMS program documents (i.e., program requirements documents, acquisition program baseline, business cases, and Implementation Strategy and Planning Document). It may also make acquisition program baseline change decisions that alter program performance, cost, and schedule baselines during Solution Implementation for investment programs. From an SRM viewpoint, if a baseline change is being proposed, the PMO/PST/CST may need to review and update any safety assessments that have already been completed to ensure that the new baseline does not impact the risk mitigation strategies already identified. If it does, then the predicted residual risks identified in the completed safety assessments may not be achievable, and the new predicted residual risk without these mitigations implemented may be unacceptable. A baseline change could affect the risk mitigation strategies already identified 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. In other words, the planned mitigations may not be in place as expected and required.
- If the performance is being re-baselined, the new requirements may be sufficiently different that the assumptions made and analyses conducted as part of previous safety

assessments may no longer apply to the point that previously identified risk mitigation strategies are no longer valid.

6.2 Program Safety Requirements for Decommissioning and Disposal

Disposal of an asset or program is part of the AMS process in the ISM phase and, as such, requires adherence to the SMS as part of its lifecycle management. In addition, decommissioning of a service provided by a program asset targeted for disposal could occur much earlier than the actual disposal and must also meet all of the SMS requirements. Programs or assets facing disposal often have their SMS requirements met by the program or asset replacing them, but this is not always the case.[20] Prior to an asset or program being decommissioned and/or disposed of, the PMO should contact the AJI Safety Case Lead to convene an SSM to determine if there are any new SMS requirements. The SSM output will indicate the need for an SRMD or SRMDM. If an SRMD is required, an SRM panel will perform a Preliminary Hazard Analysis–type assessment to determine if the NAS would be exposed to any unacceptable risk due to the disposal activity. This may include deactivation, deactivation with a replacement system, or similar considerations.

6.3 Managing Software Risk

6.3.1 Software SRM

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

- Software does not wear out. When software fails, it is due to a design or implementation defect that has always existed.
- Software fails without warning. There are no such things as intermittent failures, brownouts, etc. Software fails in the field because it is subjected to inputs or combinations of inputs that were not anticipated and/or were not tested during development. Latent defects may have existed before release of the product and may only be triggered or recognized once they are in broad use.
- Software can be more complex than hardware. It is common for device software to be hundreds of thousands or millions of lines of code long. Device software may also be integrated with commercial off-the-shelf systems software, such as operating systems that can easily reach similar sizes.
- It is difficult to test all of the software in a device, and nearly impossible to test all combinations of inputs and branching.
- Software is easily changed. Attempts to make last-minute corrections can lead to undesired results.
- Seemingly insignificant changes in one area of software functionality can lead to defects in unrelated areas of functionality.

[20] The following would seem intuitive: (1) Once a NAS asset is removed from service, it is no longer a part of the flight day decision-making process. (2) Even if it 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 (and not intuition-driven) process that still must be conducted.

6.3.2 Software Development Assurance

RTCA DO-278A establishes an approval liaison process that has similarities to the RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, certification liaison process for aircraft software. However, there are also fundamental differences to be considered. In the case of the aircraft, the applicant is external to the FAA and is regulated by the certification authority. In the case of CNS/ATM systems, the applicant is internal to the FAA, while the software developers are external to the FAA. If it is determined through the safety analyses that the CNS/ATM software can affect systems on board the aircraft, then the assigned Development Assurance Level (DAL) must be acceptable to the aircraft certification authority. The certification authority must also be allowed to provide input to the approval process.

6.3.2.1 Determining the DAL

For software, risk assessment is performed to assign the proper level of rigor to be applied during the software design, development, and testing. An appropriate level of rigor is necessary to ensure confidence that the software will not cause or contribute to a system hazard. Determining the software DAL related to a hazard is a three step process:

1. Determine a hazard’s severity classification. A hazard's severity is based on the expected effect(s) of the hazard. Severity is classified according to the severity classifications defined in the ATO SMS Manual.
2. Assign the DAL in accordance with the severity classification. A DAL for software should be assigned according to the severity of the hazard to which the software contributes.
3. Determine if architectural considerations warrant a level different from the initial level. In some cases, architectural mitigation may justify a revision of the DAL to a less stringent classification. Guidance for software architectural mitigation can be found in RTCA DO-278A.

Software that can be a causal factor for hazards must be evaluated to determine the appropriate software assurance level per DO-278A. Additionally, software design safety requirements, as well as development and testing processes, must be at an assurance level proportional to the degree to which the software product can contribute to a system hazard.

ATO-SG 14-01, *Development Assurance for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*, provides more detail on determining the correct DAL.

6.3.2.2 Gap Analysis

Many of the non-airborne CNS/ATM systems have been developed and fielded using software development processes other than RTCA DO-278A, such as Institute of Electrical and Electronic Engineers Standard 12207, “Standard for Information Technology – Software Lifecycle Processes,” or vendor’s best practices. This creates a potential problem when incorporating DO-278A software assurance requirements for additions to and/or modifications of these non–DO-278A legacy systems. For these cases, a DO-278A Gap Analysis is used to evaluate how the non–DO-278A processes adhere to the intent of DO-278A.

A DO-278A Gap Analysis should be conducted for each function within the system/software being evaluated. DO-178C/DO-278A guidelines ensure a specific software design and development assurance from the systems safety assessment process, one that is based on software architecture and functions.

The DO-278A Gap Analysis provides a basis for addressing any shortfalls from the required DO-278A objectives. The Gap Analysis must be provided to the approval authority[21] and included as an attachment to the Plan for Software Aspects of Approval (PSAA).[22]

It should be noted that conducting the DO-278A Gap Analysis is not a specific responsibility of the PST. Typically, this effort is led by the ATO PMO acquiring the new system or proposing changes to an existing system, with help from the prime contractor conducting systems integration and the subcontractor(s) responsible for developing the software. Other key participants in the process are the DO-278A SME (someone who has qualified skills and knowledge related to software assurance, specifically related to DO-278A or DO-178C) and the Approval Authority.

ATO-SG 14-03, *Conducting a DO-278A Software Assurance Compliance Gap Analysis for Acquired NAS Systems,* provides more detail on developing a DO-278A Gap Analysis.

6.3.2.3 Software Approval Process

The software approval authority may review the software lifecycle processes and associated data at his or her discretion to confirm that a software product complies with the approval basis and the objectives of RTCA DO-278A. The software review process assists both the approval authority and the applicant in determining if a project will meet the approval basis and RTCA DO-278A objectives. The software review process does this by providing:

- Timely technical interpretation of the approval basis, RTCA DO-278A objectives, 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 software plans and procedures; and
- The opportunity for the approval authority to monitor SME activities.

The following types of software lifecycle data are related to the approval process:

- PSAA
- Software Requirements Data
- Design Description
- Source Code
- Executable Code
- Software Configuration Index
- Software Accomplishment Summary

ATO-SG 14-02, *Software Assurance Approval Guidelines for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*, provides more detail on assessing the software approval process.

[21] The approval authority is the ATO authority that accepts and/or approves software lifecycle data for the ground system. This is usually the same office that approves the related safety analyses. For CNS/ATM systems that affect the NAS, this is the ATO Chief Safety Engineer.

[22] The PSAA is the primary means used by the approval authority for determining whether an applicant is proposing a software lifecycle that is commensurate with the rigor required for the assurance level of software being developed.

6.4 Site Implementation

Order JO 6000.50 complements existing policies regarding SRM and standardizes processes for Operational Risk Management (ORM) during installation activities. Order JO 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
- Required Maintenance

Order JO 6000.50 also requires that the program office prepares a Generic Site Implementation Plan (GSIP) and conducts SRM on the GSIP itself. A GSIP is required for all construction, installation, and/or removal activities in the NAS. The GSIP contains an SRM section that provides installers and maintainers with any identified hazards, mitigations, and residual risks identified during the acquisition process, as documented in the System Safety Assessment Report or the SRMD, as applicable.

Note that operational risks may have no impact on safety, but must be considered before a system is deployed.

6.5 Legacy Systems 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 change must be assessed to determine if it will introduce/reveal any hazards or affect the safety risk level of the operation/system.

Changes to legacy systems that are initiated due to component obsolescence can be designated as a Technical Refresh. These types of changes include Service Life Extension Programs, Replacement-in-Kind programs, Facility Initiative programs,[23] and Variable Quantity programs.[24] It has been commonly accepted that a change that results in a “box-for-box” replacement of obsolete or unserviceable components containing the 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, then the full SRM process must be followed. If the change does not introduce/reveal any hazards or affect the existing safety risk level of the operation/system, then this may be documented in an SRMDM.[25] The supporting documentation must justify this decision. Refer to the ATO SMS Manual for SRMDM requirements.

Changes to legacy systems can include additional functionality or a combination of existing functionality in a way that is not present in 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 enabled by a mechanical switch in the legacy system, but is enabled by software in the

[23] A Facility Initiative program is a program associated with the new construction, replacement, modernization, repair, remediation, lease, or disposal of FAA's manned and unmanned facility infrastructure(s).

[24] 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.

[25] However, if it does, the full SRM process must be implemented as described in the SRMGSA.

Technical Refresh. If the assessment determines that there is new or combined functionality, or if there is any effect to the existing hazards or how they are controlled (including the introduction of any new hazards), then the standard SRM activities documented in the AMS, the ATO SMS Manual, and the SRMGSA are required.

The conduct of these assessments may be facilitated by examination of the program’s Concept of Operations, functional analysis, shortfall analysis, enterprise architecture products, and preliminary requirements in the pPRD. In all cases, the PST should conduct an SSM (and consult with the ATO Chief Safety Engineer, as necessary) to determine if an SRMDM is appropriate or if the program should develop an SRMD per the current AMS milestone requirements.

A program undergoing a Technical Refresh needs to comply with all aspects of the AMS and SMS processes. The requirements for each Technical Refresh are typically very streamlined or tailored when compared to the original program. For Technical Refresh programs, the PST will conduct an SSM (consulting with the ATO Chief Safety Engineer, as necessary) to identify the SMS requirements as soon as practicable. Each Technical Refresh varies in its purpose and requirements, but the SMS requirements may be minimal if the Technical Refresh’s form, fit, and function are the same as when the program first went through the AMS.

6.6 Security, Information Security, and Occupational Safety and Health

Physical security, information security, and occupational safety and health issues are only considered within the scope of the SMS if they have safety effects on the operational NAS. This is not to suggest that security- and occupational safety and health−related hazards cannot be dealt with by the appropriate authority; rather, the risk(s) associated with issues such as occupational safety, information security, operational security, physical security, cyber security, and Security Certification and Authorization Packages must be transferred to the appropriate authority. In most security cases, this is the Office of Information Systems Security. For occupational safety and health hazards (including fire and life safety), Environmental and Occupational Safety and Health (EOSH) Services is the appropriate authority for the transfer of risk.

Examples of security hazards such as spoofing, jamming, intentional misuse, or malicious actions would need to be transferred to the appropriate authority, even though they may be considered outside the scope of the SMS. If a safety assessment reveals security or occupational safety and health hazards, those hazards must be documented and transferred to the appropriate authority.

6.7 Program Risk Management

Program risk management is applied throughout the 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 is found in section 4.13 of the AMS.

Program risk management and SRM have separate focuses. For instance, cost and schedule impacts are not factored into a safety assessment, but are a 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 affecting program cost or schedule by delaying or stopping implementing activities. Knowledge of SMS policies and proper planning will help the PM and PST to minimize any SRM impacts to cost and schedule. The AJI Safety Case Leads can also assist in this area.

7 Equivalent Processes

Every program is different in scope, complexity, criticality, and resources. In recognition of these differences, programs may use other equivalent processes when conducting the hazard analysis portion of SRM. While these processes may be used, the minimum requirements set forth in the SRMGSA must still be met. An equivalent safety analysis may be used under the following conditions:

- The equivalent process must meet the minimum requirements for the safety analysis outlined in the SRMGSA.
- The use of equivalent processes must be discussed with and approved by the ATO Chief Safety Engineer and documented as part of the SSM process.
- The equivalent process must be described in the PSP.

8 SRM Documentation, Approvals, and Tracking

8.1 SRMDs

An SRMD is a report, or a series of reports, that describes the SRM process with regard to a proposed change or investment. An SRMD documents the safety risk analyses that were performed and the findings that support whether the proposed change or investment is free of unacceptable risk. The SRMD is a compilation of the SRM documentation completed to date. As such, the SRMD will expand with each assessment or analysis as a product moves through the AMS lifecycle. When it is determined at the SSM that specific safety analyses are required, the analyses are documented and become part of the SRMD. Each PST must maintain an SRMD as a record of the progress of the product. SRMDs are reviewed by the AJI Safety Case Lead and must be approved by the ATO Chief Safety Engineer.

8.2 SRMDMs

If an acquisition change is not expected to introduce safety risk into the NAS, there is no need to conduct further safety analysis; instead, the PMO/PST must document this determination, along with the justification as to why the change is not subject to additional SRM assessments, in an SRMDM. The SRMDM must also include a description of the NAS change and affected hardware; software; and/or operational NAS equipment, operations, and/or procedures. The SRMDM must also include a justification for the determination that there are no hazards, or any expected change to the current risk associated with the implementation of the NAS change. A designated management official from each affected Service Unit must approve the SRMDM. As with SRMDs, SRMDMs related to NAS acquisition changes are reviewed by the AJI Safety Case Lead and must be approved by the ATO Chief Safety Engineer.

8.2.1 Non-NAS Programs

When an acquisition will have an effect on the safety of the NAS, SRM must be conducted and documented throughout the lifecycle of the product or service, in accordance with the SMS (i.e. the SRM is not a requirement when there is no safety effect on the NAS). In the AMS, AJI is designated as the responsible office for determining whether an acquisition affects the safety of the NAS. If AJI has determined there is no safety effect, then the ATO Chief Safety Engineer will provide documented notification to the JRC Secretariat accordingly. Programs should contact the AJI Safety Engineering Team Manager to initiate discussions if they believe they will be exempt from SMS requirements.

8.3 Peer Review Process

A peer review of SRM documentation determines if it meets SMS policy guidelines and the FAA's safety objectives. A peer review provides for an independent assessment of the documented analysis by multiple people with varying knowledge and experience. This helps ensure that the analysis is technically accurate and makes operational sense (i.e., the safety hazards, causes, effects, and mitigations are appropriate).

All acquisition-related SRM documentation, including SRMDs, SRMDMs, PSPs, or CapSAs,[26] must undergo a peer review before being submitted to the ATO Chief Safety Engineer for approval. The SRM document is submitted to the AJI Safety Engineering Team Manager who assigns an AJI Safety Case Lead to coordinate the peer review process. The AJI Safety Case Lead must first review the SRM documentation to determine if it meets all applicable SRM requirements and guidelines of the ATO SMS Manual and the SRMGSA. However, if the SRM documentation is being submitted through the AJI Safety Case Lead, this step may have already occurred. If the AJI Safety Case Lead determines that the SRM documentation is not ready for a peer review, it is returned to the originator with recommendations for resolution.

The AJI Safety Case Lead distributes the SRM documentation for peer review and comments according to the guidelines in the SRMGSA and internal AJI operating procedures. After comments are received and collated, the AJI Safety Case Lead then works with the PST or CST to generate written responses to originating commenters. The AJI Safety Case Lead then determines acceptance from the originating commenters, recording any discrepancies associated with partial acceptance or non-concurs. Acceptance can be determined by a combination of e-mail, phone conversations, and meetings. Meetings are preferable when comments and/or responses are complex. A final compilation of all comments and their dispositions is provided to all reviewers. Figure 8.1 shows a high-level flow diagram of the peer review process.

[26] CapSA Reports are co-approved by ANG.

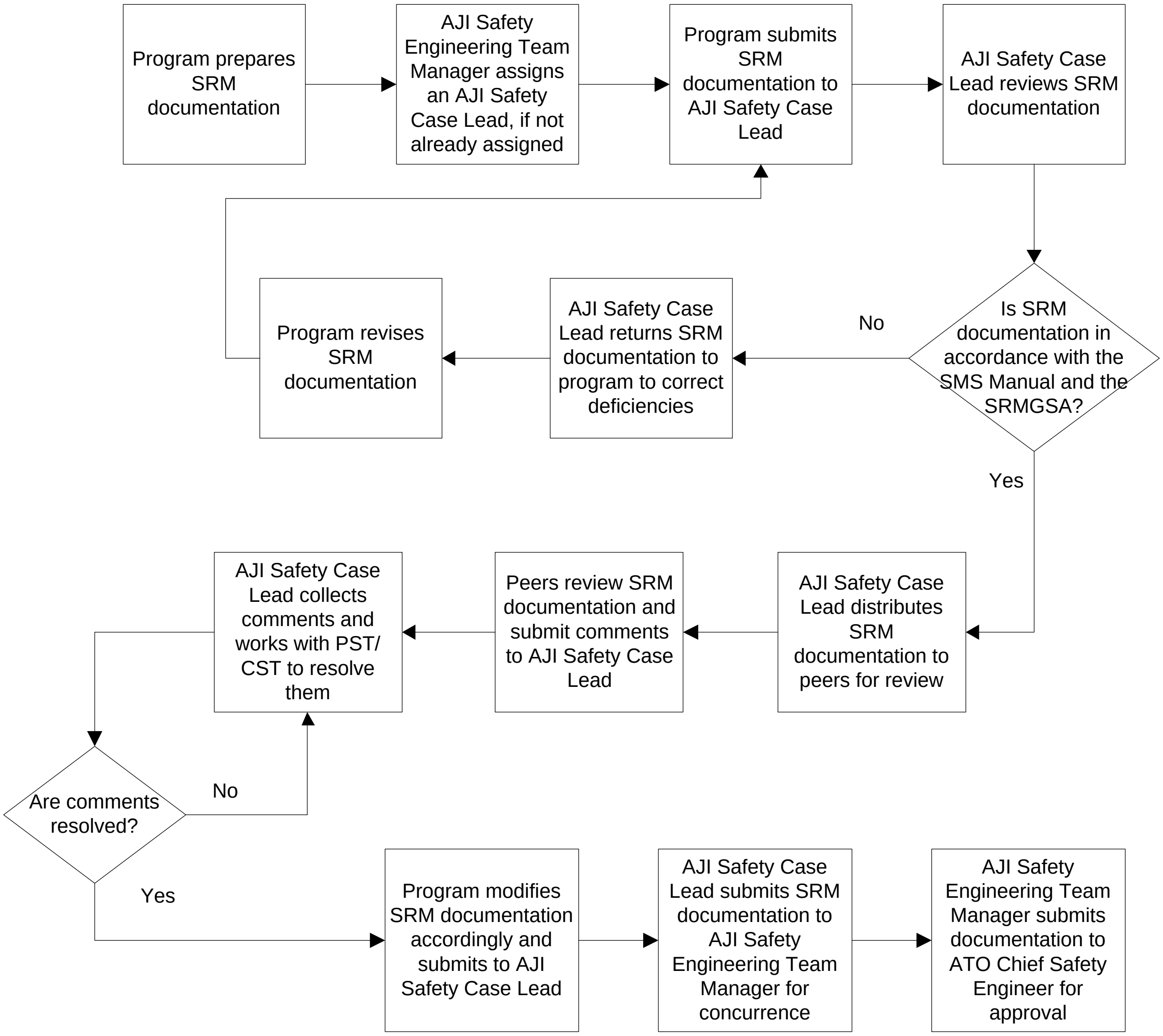

Program prepares SRM documentation
AJI Safety Engineering Team Manager assigns an AJI Safety Case Lead, if not already assigned
Program submits SRM documentation to AJI Safety Case Lead
AJI Safety Case Lead reviews SRM documentation
Is SRM documentation in accordance with the SMS Manual and the SRMGSA?
No
AJI Safety Case Lead returns SRM documentation to program to correct deficiencies
Program revises SRM documentation
Yes
AJI Safety Case Lead distributes SRM documentation to peers for review
Peers review SRM documentation and submit comments to AJI Safety Case Lead
AJI Safety Case Lead collects comments and works with PST/ CST to resolve them
Are comments resolved?
No
Yes
Program modifies SRM documentation accordingly and submits to AJI Safety Case Lead
AJI Safety Case Lead submits SRM documentation to AJI Safety Engineering Team Manager for concurrence
AJI Safety Engineering Team Manager submits documentation to ATO Chief Safety Engineer for approval

Figure 8.1: Peer Review Process Flow

Peer reviewers are designated as either primary or secondary reviewers depending on their role in the approval process, and by the following guidelines:

Primary reviewers are:

- Other AJI Safety Case Leads,
- Safety Services representatives,
- ISA Team representatives (IOA-designated programs only),
- ANG Safety and Information Security Services Division representatives,
- Representatives from offices responsible for implementing safety requirements (e.g., Aircraft Certification), and
- Representatives from offices responsible for accepting safety risk.

Secondary reviewers are:

- Quality Control Group representatives from the Service Center;
- AOV Safety Management Oversight Division representatives;
- Human Factors representatives;
- EOSH Services representatives; and
- Representatives from other AJI offices, as required.

The peer review timeline is dependent upon various factors including, but not limited to, the complexity of the safety analysis, the number of stakeholders involved, new technologies involved, prior reviews, and projected JRC decision dates. The minimum time periods allocated for each sub process are depicted in table 8.1. These times can be reduced if draft versions were already reviewed and increased when necessary. If comments cannot be resolved to the satisfaction of the original commenter, then they are identified as issues for inclusion in the final briefing package provided to the ATO Chief Safety Engineer upon recommendation for approval by the AJI Safety Engineering Team Manager.

Table 8.1: Peer Review Process Timeline

Peer Review Timelines	
Sub-process	**Minimum Time Period**
If an AJI Safety Case Lead has not yet been involved in the assessment, he or she reviews the document to determine if it is ready for peer review	7 working days
Initial peer review and comment period	11 working days from day of distribution
AJI Safety Case Lead collates comments and works with program office to generate and distribute program responses to commenters	7 working days
Commenters provide concurrence, non-concurrence, or counter proposal	5 working days
Disposition of outstanding comments	Not defined

8.4 Approval Authorities and Coordination Requirements

The ATO SMS Manual and the SRMGSA contain the guidance and coordination requirements for the review, approval, and risk acceptance of SRM documentation contained completely within a Service Unit, across multiple Service Units, or across multiple LOBs. SRM documentation will not be submitted to the ATO Chief Safety Engineer for approval until after it has gone through the peer review process, as discussed in section 8.3. The ATO Chief Safety Engineer is also the approval authority for PSPs, as well as the representative that informs the JRC and ISD Secretariats' groups as to which programs are compliant with SMS requirements.

8.5 Safety Management Tracking System

AJI will provide and manage a web-based safety management tracking system designed to track all SRM efforts and approvals from project initiation to the completion of the monitoring plan. The use of a safety management tracking system is required for all safety assessments and analyses, beginning with the OSA and continuing throughout the product's lifecycle. Its primary purpose is to track hazards and their mitigations. The safety management tracking system houses SRMDMs, SRMDs, and their associated safety analyses, allowing change proponents and SRM panels to use this information for similar efforts. Additionally, the safety management tracking system tracks the implementation and ongoing monitoring activities, which enables change proponents to assess and track predicted residual risk.

9 Safety Requirements in the AMS Lifecycle

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 9.1 and described in section 9.1.

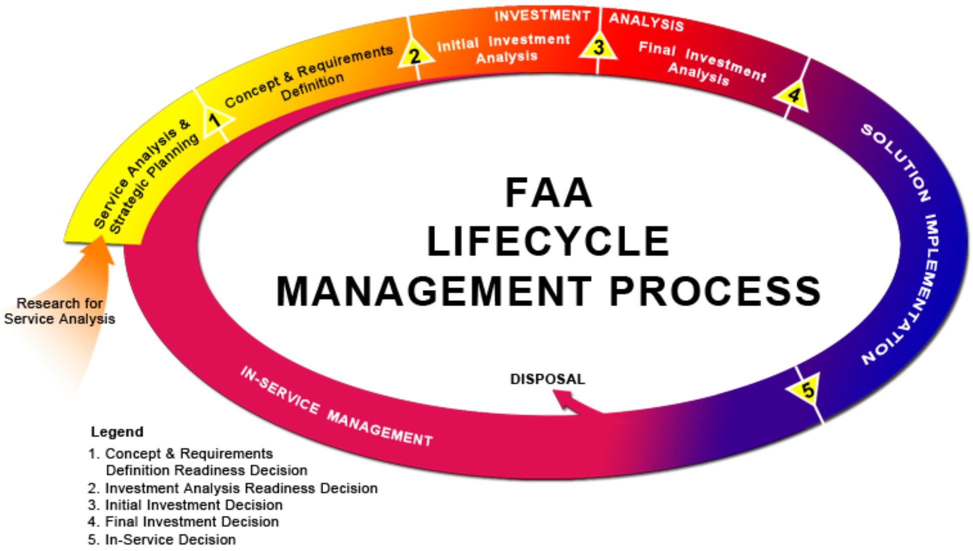

INVESTMENT
ANALYSIS
Service Analysis & Strategic Planning
1
Concept & Requirements Definition
2
Initial Investment Analysis
3
Final Investment Analysis
4
SOLUTION IMPLEMENTATION
5
DISPOSAL
IN-SERVICE MANAGEMENT
Research for Service Analysis
FAA LIFECYCLE MANAGEMENT PROCESS
Legend
1. Concept & Requirements Definition Readiness Decision
2. Investment Analysis Readiness Decision
3. Initial Investment Decision
4. Final Investment Decision
5. In-Service Decision

Figure 9.1: FAA Lifecycle Management Process

9.1 The FAA Lifecycle Management Process

Integrating SRM into the AMS process is a major objective of the SRMGSA. This objective can be achieved by accomplishing SRM tasks using the correct systems safety tools and techniques at the appropriate time to support the decisions made in the lifecycle phase. These tasks are mainly performed by the ATO PMO and result in products packaged in SRMDs, which are reviewed and approved prior to a JRC decision.

The circular representation in figure 9.1 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 AMS policy contains detailed information on the Lifecycle Management Process.

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

Table 9.1 shows when and by whom the various SMS-related tasks should be completed. Appendix C provides further details of the specific program safety requirements by acquisition phase.

Table 9.1: Safety Analysis Decision Chart

Acquisition Phase	AMS Decision Point	Type of Analysis Required	Documentation Needed*	Responsibility for Preparation
Service Analysis and Strategic Planning	Not Applicable	Capability Safety Assessment (CapSA)	– CapSA Report***	ANG/AJI
Concepts and Requirements Definition	Investment Analysis Readiness Decision	Operational Safety Assessment	– SRMD o OSA – Safety requirements input to preliminary Program Requirements Document – Input into the Enterprise Architecture Safety Plan – Input into the Investment Analysis Plan	ANG / ATO PMO
Initial Investment Analysis	Initial Investment Decision	Comparative Safety Assessment (CSA)	– Update to existing SRMD: o CSA – Program Safety Plan (PSP) – Incorporation of results into Business Case Analysis Report – Briefing to the Joint Resources Council in SRMGSA format – Initial Implementation Strategy and Planning Document (ISPD)	ATO PMO
Final Investment Analysis	Final Investment Decision	Preliminary Hazard Analysis (PHA)**	– Update to existing SRMD: o PHA – Update to existing PSP – Final Program Requirements Document – Final ISPD	ATO PMO
Solution Implementation	In-Service Decision	Sub-System Hazard Analysis (SSHA), System Hazard Analysis (SHA), Operating & Support Hazard Analysis (O&SHA), and others, as defined in the PSP; Independent Operational Assessment (IOA)	– Updates to existing SRMD: o SSHA o SHA o O&SHA o System Safety Assessment Report (includes Safety Action Records and Safety Requirements Verification Table) – Update to existing PSP – The In-Service Review Checklist	ATO PMO / AJI (IOA only)
In-Service Management	Post-Implementation Review	Review SRMD monitoring plan; Post-Implementation Safety Assessment	– SRM section of Post-Implementation Review Report	ATO PMO

*The ATO Chief Safety Engineer reviews and approves all safety documentation.
**Conducted on the down-selected alternative.
***See appendix B for guidance.

Appendix A

Guidance for Preparing and Implementing Program Safety Plans

Guidance for Preparing and Implementing Program Safety Plans

1 Purpose

This guidance gives a process consistent with the Air Traffic Organization (ATO) Safety Management System (SMS) for preparing and implementing Program Safety Plans (PSPs) for systems that will be fielded in the National Airspace System (NAS) and were acquired under the Federal Aviation Administration (FAA) Acquisition Management System (AMS).

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in FAA orders. It reflects updates to the ATO SMS Manual and the Safety Risk Management Guidance for System Acquisitions (SRMGSA), both of which provide guidance on fulfilling requirements set forth in Order JO 1000.37, *Air Traffic Organization Safety Management System*, and the FAA AMS.

3 Background

A PSP is the government's integrated management plan for conducting the system safety program for a particular project or program. By executing this plan, the government ensures compliance with the provisions of the ATO SMS Manual, the SRMGSA, and the AMS. Use of a PSP also ensures that an acceptable level of safety consistent with mission requirements is designed into the system.

Under the leadership of a Program Manager (PM),[1] a Safety Team (either a Capability Safety Team (CST) or a Program Safety Team (PST)[2]) must develop and tailor a PSP that details the specific safety needs and Safety Risk Management (SRM) requirements of the program and update the PSP as the program matures and information changes. This PSP forms the basis of the prime contractor's corresponding Systems Safety Program Plan (SSPP), which is typically contractually required as a deliverable. The prime contractor's SSPP, when approved by the government, binds the contractor to a system safety program that must be consistent with the government's PSP.

The PSP also stands as the PM's agreement with ATO Safety and Technical Training (AJI)[3] to conduct a safety program that is consistent and compliant with the ATO SMS. It defines the roles and responsibilities of the PM / Safety Team members as they implement the system safety program. As such, the PSP must describe:

- The safety program that applies to each project, subsystem, and interface to support program activities and SMS/SRM requirements;
- The SMS/SRM responsibilities of the PM / Safety Team; and
- Planned SRM efforts.

[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 will transfer from the Assistant Administrator for the Office of NextGen to ATO Mission Support Services / ATO Program Management Organization / ATO Technical Operations Services.

[2] The roles of the CST and the PST are defined in the SRMGSA. As with program management, the leadership and composition of these teams may change as a program proceeds through the AMS lifecycle.

[3] Or more specifically, with the ATO Chief Safety Engineer, as explained in the SRMGSA.

4 Procedures

There are seven key steps in preparing/implementing a PSP:

- Identify the system safety program requirements.
- Develop a safety strategy based on these requirements.
- Translate the developed safety strategy into a PSP.
- Submit the PSP for approval and signature.
- Implement the system safety program in accordance with the PSP.
- Update the PSP, as needed.
- Monitor and review the progress of PSP implementation.

4.1 Identify the system safety program requirements.

Requirements identification is an initial step that must be conducted in order to tailor a program's safety strategy. The PM, the Safety Team, the AJI Safety Case Lead,[4] the Office of NextGen, and other stakeholders collaborate to identify the requirements and solidify them via one or more Safety Strategy Meetings (SSMs). The identification process consists of several sub-steps.

4.1.1 Review Generic Systems Safety / SMS and AMS program requirements.

The PM / Safety Team should review generic source documentation such as the AMS (specifically section 4.12), the FAA System Safety Handbook, the ATO SMS Manual, the SRMGSA, and applicable ATO and FAA orders (such as Order JO 1000.37 and Order 8040.4, *Safety Risk Management Policy*). This needs to be done to determine the prescribed safety requirements the program must meet at each acquisition milestone.

4.1.2 Review and accept high-level safety program requirements.

The Next Generation Air Transportation System (NextGen) is highly distributed[5] and interconnected in nature. For instance, within a NextGen Portfolio, there may be Operational Improvements consisting of defined increments and Operational Sustainments. All of these elements must work together to deliver operational capabilities. To provide a complete picture of the potential safety risk of fielding a particular capability, Capability Safety Assessments (CapSAs) are conducted. CapSAs facilitate integrated safety management for a capability and identify high-level safety requirements. These requirements are then distributed down to the individual increments as applicable.

The PM / Safety Team and AJI Safety Case Leads must ensure that these high-level requirements are accepted and eventually translated into specific program requirements that are included as part of the overall program safety strategy. They must also be able to trace their specific safety requirements back to the portfolio level.

[4] An AJI Safety Case Lead is assigned by AJI to assist acquisition programs in meeting applicable SRM requirements. His or her roles and responsibilities are delineated in the SRMGSA.

[5] A distributed system consists of a collection of autonomous computers linked by a computer network and equipped with distributed system software.

4.1.3 Identify mechanism for tracking and monitoring program hazards.

Order JO 1000.37 requires that all identified safety hazards and their safety risks be recorded in a database. The PM / Safety Team must use a safety management tracking system provided by AJI[6] to enter data for new safety analyses before beginning the monitoring process. Enter all hazards into the safety management tracking system, including those with low risk. The PM / Safety Team must ensure that personnel have been trained to use this system and that safety management tracking system use is integrated into the system safety program.

4.1.4 Identify developmental assurance requirements.

Development assurance is required for systems containing software whose anomalous behavior can cause or contribute to a failure condition with safety-related consequences. Software is a hazard cause and may or may not be a significant contributor to the hazard under consideration. It is highly recommended that development assurance be conducted in accordance with RTCA DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*.[7] Since the assurance level can have a significant impact on development costs, it is important to accurately evaluate the software's contribution to a hazard. The methodologies used for this evaluation should be included in the PSP.

4.1.5 Identify Post-Implementation Review safety requirements.

A Post-Implementation Review (PIR) is an evaluation tool used to assess results of an investment program against baseline expectations 6 to 24 months after it goes into operational service. Its main objective is to determine if the program is achieving expected performance and benefit 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. A PIR strategy is developed during the AMS lifecycle during the Final Investment Analysis and must include appropriate safety considerations, which should be incorporated into the PSP.

4.1.6 Develop a nominal safety program schedule.

Given that there must be an approved PSP in place at each major decision point of the acquisition process after the Concept and Requirements Definition phase (i.e., Investment Analysis Readiness Decision, Initial Investment Decision, Final Investment Decision, and In-Service Decision), the PM / Safety Team must develop a nominal safety program schedule consistent with the Joint Resources Council (JRC) decision points.

4.2 Develop a safety strategy based on the identified program requirements.

Given the identified program safety requirements, the PM / Safety Team then develops 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 Safety Case Lead and in consultation with the ATO Chief Safety Engineer, if necessary (particularly if a large amount of document tailoring is being considered).

4.2.1 Prepare a Safety Strategy Worksheet (SSW).

To prepare for the SSMs, the PM / Safety Team must first prepare an SSW. At a minimum, this worksheet must contain the following information:

- System/program name and previous program name, if any

[6] Information about the safety management tracking system can be found in the SRMGSA.

[7] Other acceptable alternatives exist and can be used with approval from the ATO Chief Safety Engineer.

- Short system description
- System/FAA/external interface(s)
- Interdependencies
- Changes to legacy systems, if any
- Name / phone number of key individuals: PM, leader of the Safety Team, AJI Safety Case Lead, applicable Service Unit Subject Matter Experts (SMEs), and a DO-278A SME[8]
- Where the program is in the AMS lifecycle
- Any plan for combining JRC decision points
- Whether alternative solutions will be proposed
- Proposed dates of the JRC reviews and Initial Operational Capability / In-Service Decision
- Impact of the system on the NAS, separation, navigation, communications, and aircraft
- Potential safety risk of the system to the NAS
- A listing of any safety assessments completed to date and a summary of any significant safety findings
- Traceability to a NextGen Portfolio, including any requirements allocated from the portfolio
- Independent Operational Assessment (IOA) designation, if applicable

4.2.2 Set up and hold the first SSM.

The purpose of this meeting is to review the SSW to:

- Ensure the PM / Safety Team, the AJI Safety Case Lead, and other stakeholders have a common understanding of the program's safety requirements;
- Outline the safety documentation required; and
- Set a schedule for document preparation, coordination with other lines of business as needed, and approval.

The outcome of this meeting will be a safety strategy that is mutually agreed upon by the PM / Safety Team, the AJI Safety Case Lead, and other stakeholders.

4.3 Translate the safety strategy into a plan.

The PSP supports the entire range of activities in every phase of the program. The PM / Safety Team must develop the safety strategy that was agreed to into a plan that includes at a minimum the following information:

- Program scope and objectives
- Program safety organization
- Program stakeholders

[8] An RTCA DO-178 Designated Engineering Representative would be considered a DO-278A SME.

- Safety program milestones
- General safety requirements and criteria, including their traceability to NextGen Portfolios
- Hazard analyses to be performed
- Hazard tracking system processes to be used
- Safety data to be collected
- Safety requirements management[9]
- Safety management of changes to program changes (e.g., scope, design, schedule)
- Safety training required
- Safety interfaces with development engineering, contractors, management, and other specialty engineering groups
- Interfaces with other PSPs
- IOA designation, if applicable

4.4 Submit the PSP for approval and signature.

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

- The leader of the Safety Team prepares, signs, and submits the PSP to the PM for approval.
- If acceptable, the PM signs the PSP and returns the document to the leader of the Safety Team for further coordination, as necessary.
- The PSP is submitted to the AJI Safety Case Lead for coordination, approval, and signature by the ATO Chief Safety Engineer.

4.5 Implement the system safety program in accordance with the PSP.

Once the document is approved, it becomes the PM's responsibility to implement the PSP as agreed to with the support of the Safety Team. The PM must also coordinate with the prime contractor to ensure that SSPP-defined safety efforts are being implemented and support the safety tasks in accordance with PSP.

4.6 Update the PSP as needed.

The PSP is a living document that must be updated by the PM / Safety Team as circumstances change (e.g., different acquisition phases, changes to the program structure/management team, program financial profile, program approach). The PSP must be reviewed prior to each AMS milestone decision. If agreements made in the original PSP need to be amended, the AJI Safety Case Lead must resubmit the revised PSP to the ATO Chief Safety Engineer for approval.

[9] 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 to NAS capabilities.

4.7 Monitor and review the progress of PSP implementation.

The PM must ensure that the PSP is implemented per the schedule agreed to and must inform the AJI Safety Case Lead of any deviations from the plan. The PM must use the safety management tracking system as a tool to enhance his or her monitoring of the safety program. The AJI Safety Case Lead must also monitor the safety program on a regular basis, particularly as JRC milestones approach and certain required documentation needs to be approved.

Appendix B

Guidance for Conducting Integrated Safety Risk Management

Guidance for Conducting Integrated Safety Risk Management

1 Purpose

The following provides guidance for conducting Integrated Safety Risk Management (ISRM) and producing Capability Safety Assessment (CapSA) Reports or Integrated System Safety Assessment (ISSA) Reports consistent with the Air Traffic Organization (ATO) Safety Management System (SMS). It concentrates on analyses conducted within the middle tier of integrated safety management, as presented in figure B.1.

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It expands upon information presented in the Safety Risk Management Guidance for System Acquisitions (SRMGSA) and reflects updates to the ATO SMS Manual, both of which provide guidance on fulfilling requirements set forth in the current version of Order JO 1000.37, *Air Traffic Organization Safety Management System*.

3 Background

3.1 Operational Capabilities and Integrated Safety Management

3.1.1 Operational Capabilities

An operational capability is a collection of service improvements known as Operational Improvements (OIs), which may be coupled with Operational Sustainments (OSs). OIs and OSs are packaged in an integrated fashion during the Service Analysis and Strategic Planning phase of the Acquisition Management System (AMS) lifecycle management process, and create new or modify the performance of existing capabilities to achieve a desired outcome or benefit. An operational capability may be composed of OIs and OSs from one or more services.

3.1.2 Operational Capability Portfolios

Section 1.2.4.2 of the FAA AMS policy, Operational Capability Portfolios, authorizes the Next Generation Air Transportation System (NextGen) Management Board (NMB) to establish operational capability portfolios to achieve priority National Airspace System (NAS) performance and operational goals. An operational capability portfolio may contain material (e.g., hardware or software deliverables) and non-material (e.g., airspace redesign or procedures) components.

3.1.3 Operational Capability Integration Plans

An operational capability integration plan defines the critical interdependencies between investment increments, how they will be managed, and their interaction with each other and the overall portfolio. The executives responsible for each investment increment of an operational capability portfolio approve the plans.

3.1.4 Integrated Safety Management

Operational capabilities are reflective of the increasingly complex, interactive, and interrelated systems in the NAS. Successful implementation of these capabilities may depend on changing systems, such as the FAA Telecommunications Infrastructure, or implementing systems, such as Automatic Dependent Surveillance − Broadcast. Development and implementation can also be affected by other internal and external factors, such as program interdependencies, realignment of priorities, or concept validation work.

These interdependencies call for an integrated approach to safety management. The goal of integrated safety management is to eliminate gaps in safety analyses by assessing NAS equipment, operations, and procedures across three planes: vertical, horizontal, and temporal. The vertical plane is hierarchical, providing assessments from a specific project up to the NAS-level system of systems of which the project is a part. The horizontal plane spans organizations, programs, and systems. Finally, the temporal plane attempts to eliminate safety gaps across program and system implementation timelines.

3.1.5 Integrated Safety Risk Management

Figure B.1 depicts the potential scope and level of Safety Risk Management (SRM) required. It shows how safety assessment responsibilities may be divided within the NAS, reflecting the idea that an increase in integration requires a corresponding increase in collaboration.

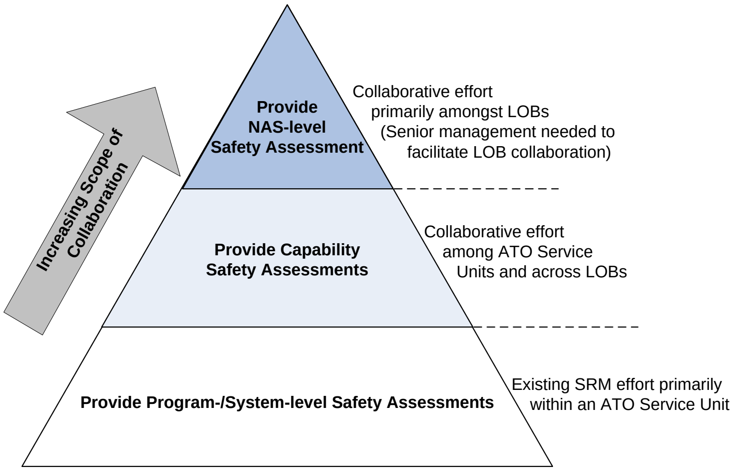

Increasing Scope of Collaboration
Provide NAS-level Safety Assessment
Collaborative effort primarily amongst LOBs (Senior management needed to facilitate LOB collaboration)
Provide Capability Safety Assessments
Collaborative effort among ATO Service Units and across LOBs
Provide Program-/System-level Safety Assessments
Existing SRM effort primarily within an ATO Service Unit

Figure B.1: Three Tiers of Integrated Safety Management

The middle tier of this framework is the capability/concept level, which involves conducting ISRM. It more fully identifies and characterizes NextGen capabilities by providing a safety risk perspective on proposed capabilities and possible hazards that may arise from the interaction of programs associated with OIs, OSs, and other increments. It also addresses how integration into the NAS Enterprise Architecture affects the interactions of related systems, including legacy systems, and their accompanying risks.

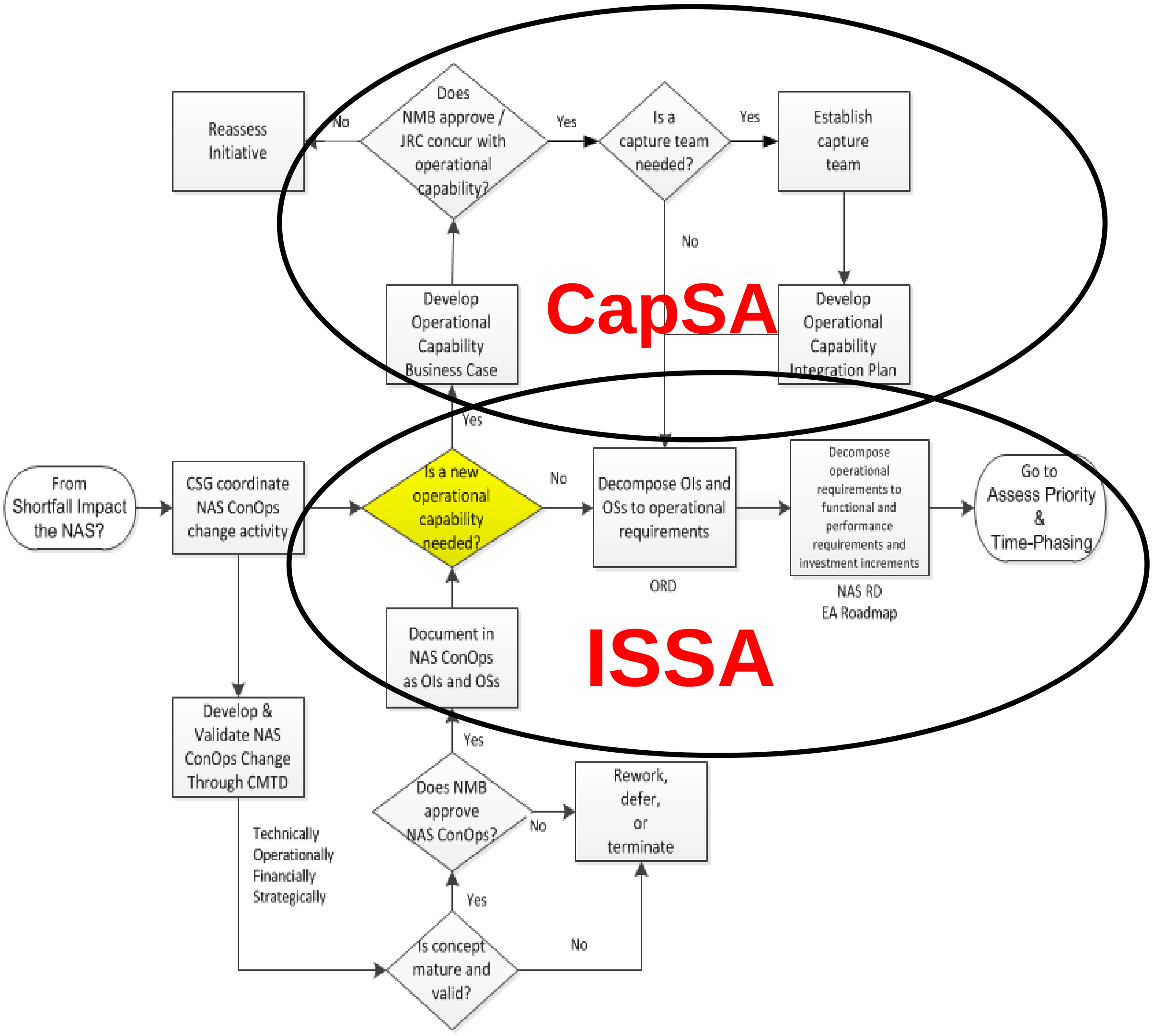
3.2 Rationale for Conducting Integrated Safety Risk Management

Prior to the Investment Analysis Readiness Decision (IARD) phase of the AMS, physical architectures and integration plans are normally not well defined, so detailed hazard analyses are not always needed. However, capability/concept safety concerns and integration issues may have enough definition to produce valuable information that should be used to develop scenarios for the modeling and simulation. Including a comprehensive safety analysis in this development will help the ATO and the Office of NextGen identify and understand new integrated hazards, as well as gather data as the capability evolves and moves through the AMS lifecycle.

Safety analysis may impact the feasibility of a capability/concept. The magnitude of safety concerns identified early during development may impact later investment and development decisions. Furthermore, early safety analysis will support the transition of the capability/concept to an implementing organization, resulting in an SMS-compliant Operational Safety Assessment prior to the IARD.

3.3 Operational Capability Decision Point

As a capability/concept enters the Service Analysis and Strategic Planning phase of the AMS, the FAA reaches a decision point concerning the need for a new operational capability. If a new operational capability is created, the ISRM output will be a CapSA Report that will supplement the Operational Business Case and be factored into the NMB's decisions regarding the capability. The CapSA Report results may lead to requirements and hazards being allocated to new OIs and OSs and may provide input to subsequent ISSA Reports. If, however, a new capability is not created at this time and requirements and hazards are instead allocated to existing OIs or OSs, the ISRM output will be an ISSA Report alone. Figure B.2 is an AMS process flow chart that highlights this decision point and how it results in either a CapSA Report or an ISSA Report being developed.



Reassess Initiative
No
Does NMB approve / JRC concur with operational capability?
Yes
Is a capture team needed?
Yes
Establish capture team
No
Develop Operational Capability Business Case
CapSA
Develop Operational Capability Integration Plan
Yes
From Shortfall Impact the NAS?
CSG coordinate NAS ConOps change activity
Is a new operational capability needed?
No
Decompose OIs and OSs to operational requirements
ORD
Decompose operational requirements to functional and performance requirements and investment increments
NAS RD
EA Roadmap
Go to Assess Priority & Time-Phasing
ISSA
Document in NAS ConOps as OIs and OSs
Yes
Develop & Validate NAS ConOps Change Through CMTD
Technically
Operationally
Financially
Strategically
Does NMB approve NAS ConOps?
No
Rework, defer, or terminate
Yes
Is concept mature and valid?
No

Figure B.2: ISRM in the Service Analysis and Strategic Planning Phase

3.3.1 CapSA Report

Performing ISRM to produce a CapSA Report will identify the baseline operational environment, including physical, functional, and procedural aspects, across domains (e.g., air traffic control, airspace, or aircraft). CapSA Reports will detect potential operational hazards across system boundaries, outcomes (which are common among systems), and possible hazard mitigation strategies. The CapSA Report will also identify possible invalidation of assumptions / ISRM results (including the possible introduction of hazards) caused by subsequent changes to the NAS.

3.3.2 Capability Safety Team

The Capability Safety Team (CST), as defined in the SRMGSA, will prepare a CapSA Report to address the Service Analysis and Strategic Planning phases associated with the emerging capabilities to ensure that ISRM begins early in the AMS process. The initial ISRM must be performed and the CapSA Report written in time for its conclusion and recommendations to be presented to the NMB in conjunction with the operational capability business case.

As the CapSA Report is a living document, the CST will revise it, as needed. As the capability matures, assumptions, mitigations, and hazards that were initially identified may no longer be valid. If this is the case, they will need to be revised. Any revisions to the output will flow to subsequent program-level safety documents. The CST will work with safety professionals and system subject matter experts from all organizations within the ATO and other Lines of Business (LOBs). This collaboration will facilitate the understanding of safety requirements and the approach to integrated risk assessment. It will also allow for a clear definition of the required follow-up tasks that must be conducted within each LOB.

3.3.3 Safety Collaboration Team

The Safety Collaboration Team (SCT) is a chartered FAA team of safety stakeholders from multiple FAA LOBs that supports the development and advancement of ISRM. The SCT will raise awareness of integrated safety issues and enhance risk-based decision making. The SCT is responsible for:

- Overseeing the ISRM process.
- Providing and facilitating clear, precise processes and methodologies to conduct ISRM.
- Appointing Integrated Safety Teams (ISTs) to conduct ISRM to produce an ISSA Report.
- Providing a CST or IST with enterprise-level safety information to assist with the identification of safety trends or potential safety issues.
- Leveraging CapSA Report / ISSA Report information to influence enterprise decision making (e.g., OIs and NAS Enterprise Architecture products).
- Researching and developing enterprise-level safety information to assist with the identification of safety trends or potential safety issues and recommending solutions using toolsets such as the Aviation Safety Information Analysis and Sharing, System Safety Management Transformation, or Human Performance Modeling and Hazard Traceability Views.
- Supporting the development of the NextGen Safety Portfolio.

3.3.4 Integrated System Safety Assessment Report

Performing ISRM to produce an ISSA Report differs from using the process to produce a CapSA Report in that the scope is not fixed around a capability. The ISSA Report is not an AMS requirement; only the SCT can request that it be produced. The purpose of an ISSA Report is to identify the safety issues that may eventually be categorized as hazards early in the lifecycle, as well as to identify unmanaged risks in safety analyses by assessing across the three planes. The ISSA Report will provide safety/risk information to SRM processes such as CapSA- and program-level safety assessments. Unlike a CapSA, the ISSA might only be performed once and therefore, not be iteratively updated.

3.3.5 Integrated Safety Team

The IST is appointed by the SCT to conduct ISRM and produce ISSA Reports. The IST will be composed of select representatives from the SCT with specific knowledge or expertise in the subject area of safety that is under consideration. As a sub-team of the SCT, the IST will have access to safety professionals from all stakeholder LOBs to foster the integrated safety management approach. The IST will begin performing ISRM to produce an ISSA Report early in a concept's lifecycle. The IST is responsible for:

- Thoroughly conducting ISRM,
- Developing a detailed ISSA Report,
- Revising the ISSA Report as the concept matures and/or the ISSA Report safety issues are integrated into program safety documents,
- Presenting ISRM recommendations to the SCT, and
- Participating in ATO Safety and Technical Training's safety case peer review process to ensure the alignment of program-level SRM Documents with ISRM recommendations.

4 Procedures

The outputs of the middle tier of ISRM are CapSA Reports / ISSA Reports, which are broader in scope than those assessments conducted at the program/system level and thus require guidance beyond the current SRM process described in the ATO SMS Manual. Figure B.3 depicts the overall process flow in the context of existing SRM processes. The blue boxes titled "Hazard Integration Analysis" and "Hazard Integration Analysis Process" show how the CapSA and ISSA fit within the full spectrum of ISRM. Output from the CapSA and ISSA influences the scope of the safety analysis at the program level, and the peer review process (as discussed in the SRMGSA) provides insight into how the outputs are incorporated into the program-level safety analysis. Figure B.4 provides a more detailed view of the analysis and guidance development process identified in figure B.3. Both of these processes are iterative in nature.

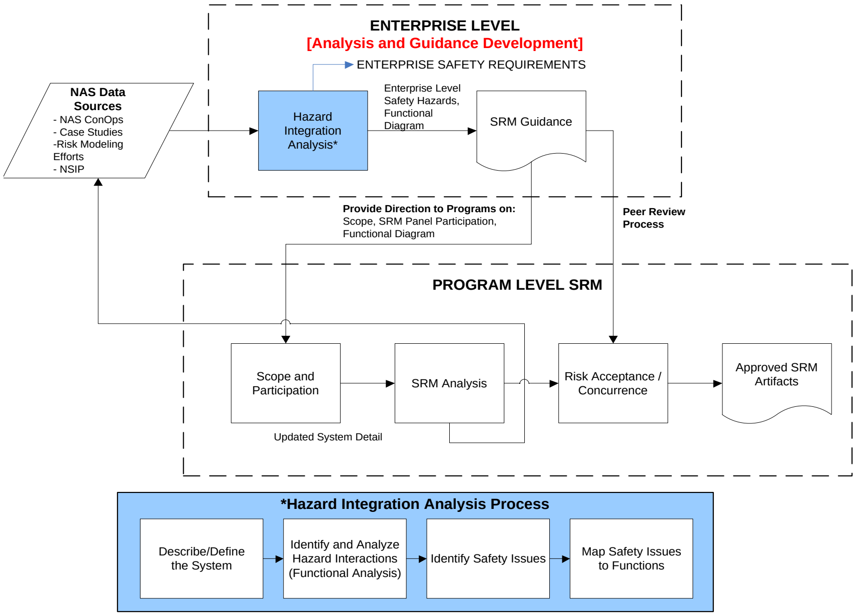

ENTERPRISE LEVEL
[Analysis and Guidance Development]
ENTERPRISE SAFETY REQUIREMENTS
NAS Data Sources
- NAS ConOps
- Case Studies
-Risk Modeling Efforts
- NSIP
Hazard Integration Analysis*
Enterprise Level Safety Hazards, Functional Diagram
SRM Guidance
Provide Direction to Programs on:
Scope, SRM Panel Participation, Functional Diagram
Peer Review Process
PROGRAM LEVEL SRM
Scope and Participation
SRM Analysis
Risk Acceptance / Concurrence
Approved SRM Artifacts
Updated System Detail
*Hazard Integration Analysis Process
Describe/Define the System
Identify and Analyze Hazard Interactions (Functional Analysis)
Identify Safety Issues
Map Safety Issues to Functions

Figure B.3: Overall ISRM Flow

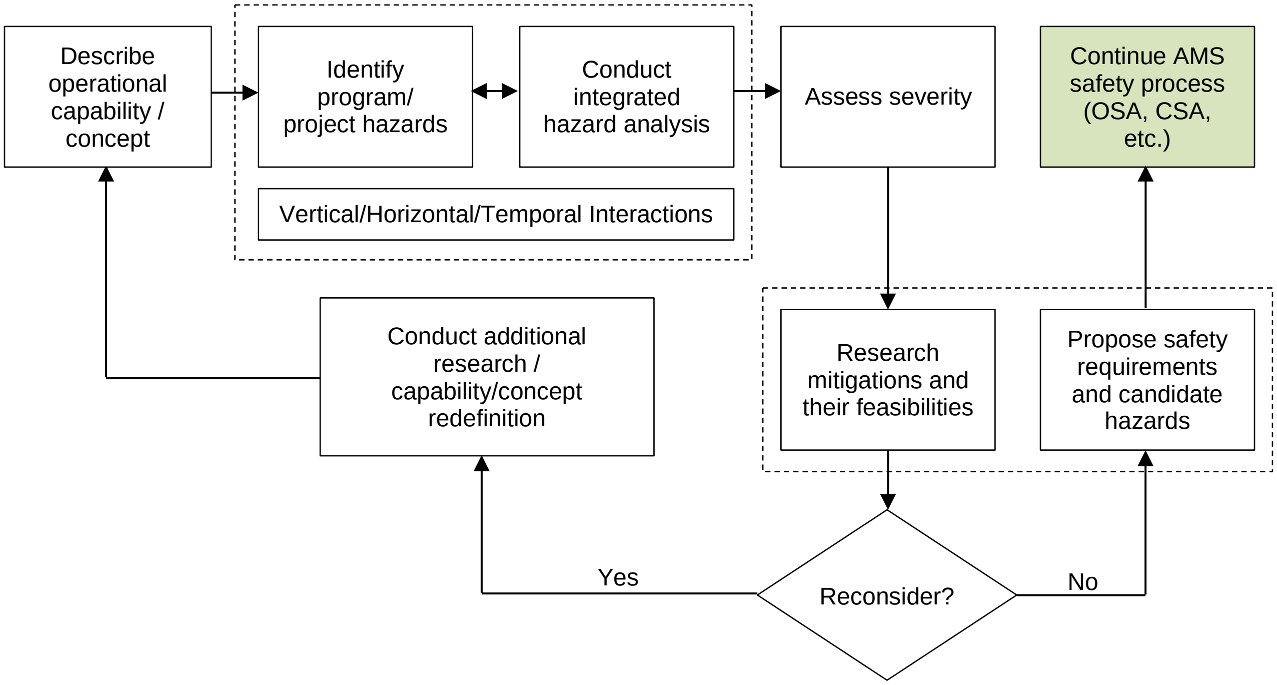

Describe operational capability / concept
Identify program/ project hazards
Conduct integrated hazard analysis
Vertical/Horizontal/Temporal Interactions
Assess severity
Continue AMS safety process (OSA, CSA, etc.)
Conduct additional research / capability/concept redefinition
Research mitigations and their feasibilities
Propose safety requirements and candidate hazards
Yes
Reconsider?
No

Figure B.4: The CapSA Report / ISSA Report Process Flow

5 A Guide for Producing a CapSA Report / ISSA Report

The following gives detailed guidance on how to conduct ISRM to produce a CapSA Report / ISSA Report. Refer to figure B.4 for a process flow chart. The contents of the nine chapters of a CapSA Report / ISSA Report are detailed below.

5.1 Introduction

This chapter gives a brief overview of the ISRM about to be conducted, and should include:

- A cursory description of the capability/concept (identifying the OIs/increments that the program/project will be supporting or enabling will assist in strengthening the business case of the program, as well as the safety case);
- Identification of stakeholders / composition of assessment panel (i.e., which LOBs the capability/concept affects);
- Identification of subject matter experts (i.e., those who can knowledgeably discuss the programs/projects included in the capability/concept assessment); and
- A description of the level of detail of the upcoming assessment and its anticipated outcomes.

The following questions and the corresponding responses should be considered when describing the level of detail of the upcoming assessment:

- *Does the ISRM being conducted cover a capability/concept exploration (e.g., for capacity or efficiency enhancements)?* Perhaps no explicit safety research or outputs are necessary. Safety concerns that may arise from literature reviews, modeling, part-task simulations, and/or other development should be documented as potential research issues.

- *Does the ISRM being conducted cover a new capability/concept intended to address specific operational issues?* The safety efforts should explicitly discuss the safety issues and propose metrics to measure success.

- *Does the ISRM being conducted cover a capability/concept formulation?* The potential positive and negative safety impacts must be discussed and used as input to identify and address potential capability/concept safety issues. Hazards need only be analyzed for severity.

- *Does the ISRM being conducted cover a capability/concept development?* The safety efforts should focus on identifying and characterizing specific hazards based on the increasingly specific functional architecture and proposed operational implementation of the capability/concept to address additional integration concerns and issues. If field demonstrations are anticipated, then test Safety Risk Management Document(s) (SRMDs) should be developed, as necessary.

5.2 Describe the operational capability/concept

This chapter describes the operational capability/concept that will be discussed.

Part of describing an operational capability/concept involves the following questions:

- What OIs, OSs, and increments are involved?
- What are the timelines of the OIs, OSs, and increments involved?
- What operational scenarios are encompassed?
- What is the operational environment?
- What related data for the projects/programs must be assembled? Consider existing applicable SRMDs.
- What systems help enable this capability/concept?

The following factors, as applicable, should be considered when describing the environment:

- Physical description of the included projects/programs, including airborne, groundside, and other projects/programs;
- Functional description;
- People, hardware, software, firmware, information, procedures, facilities, services, and other support facets;
- Assumptions and constraints (internal and external to the FAA);
- Mission;
- Human interface; and
- Operational and deployment requirements.

5.3 Identify program/project hazards and conduct integrated hazard analysis

This chapter should detail the appropriate horizontal/vertical/temporal aspects across the OIs, OSs, and LOBs. These considerations should be taken into account when identifying potential hazards.

At a minimum, the assessment should answer these questions:

- Does the capability/concept provide source material as input to systems external to the NAS?
- Does the capability/concept receive source material as input from external NAS systems?
- Does the capability/concept create or require any functional interdependencies on or from external NAS systems?
- Will the capability/concept impact or cause external NAS legacy systems to change the way they currently function (e.g., levying new requirements as a result of the capability)?
- Will mitigations implemented this year be effective several years later when other systems are introduced into the NAS? Or, to look at it another way, will systems implemented this year negate mitigations implemented in previous years? Or, will the

implementation of new systems be the catalyst for introducing unexpected hazards in legacy systems?

The assessment must analyze the identified issues and group the hazards into categories such as human factors, technical, organizational, and environmental. If possible, consider the causes of the hazards and rate their significance based on their impacts as high, medium, and low. This analysis can be a task-based or simulation.

- Task-based Analysis: Were baseline tasks identified and compared to the capability/concept to determine potential safety impacts and hazards?
- Simulation Analysis: Were results from ongoing simulations used to make inferences about the capability/concept's potential operational, procedural, and equipment safety issues?

5.4 Assess the severity

In this chapter, the assembled hazard list is reviewed and the severities of the identified hazards are assessed. The basic question to answer is, "What is the hazard severity level?" It is likely that at this stage of development, only a qualitative assessment based on the potential severity of hazards can be made. (In most cases, hazard likelihood would be difficult to determine at this point.)

5.5 Research mitigations and their feasibilities

In this chapter, it is determined whether the identified hazards are being adequately addressed. Can the operational capability/concept being analyzed be modified or supplemented with sufficient mitigations to enable it to continue down the development path? In other words, are the identified hazards too large to live with? If the mitigations are sufficient, they need to be identified, and prioritized mitigation strategies must be developed. If mitigations are not sufficient, the team must conduct additional research or re-define the capability/concept. Findings and recommendations must be documented.

5.6 Provide safety requirements and candidate hazards

If the recommendation is to continue the capability/concept development without any immediate changes, then this chapter must prioritize the candidate hazards discovered and identify safety requirements that must be allocated to OIs and OSs as the operational capability/concept is further developed.

5.7 Follow-up

This chapter establishes ownership of the follow-up actions and summarizes the results of the assessment.

5.8 References

This chapter documents unpublished and published works used within the CapSA Report / ISSA Report to either support or refute statements, or to offer alternatives.

5.9 Appendices

At a minimum, appendices should include a glossary and a list of acronyms and abbreviations. Other appendices can be included, as required.

Appendix C

Specific Program Safety Requirements by Acquisition Phase

1 Introduction

The Federal Aviation Administration (FAA) executes its acquisition management policy using a lifecycle management process, which is organized into the series of phases and decision points shown in figure C.1. Further details on each phase may be found at the FAA Acquisition System Toolset (FAST) website, http://fast.faa.gov.

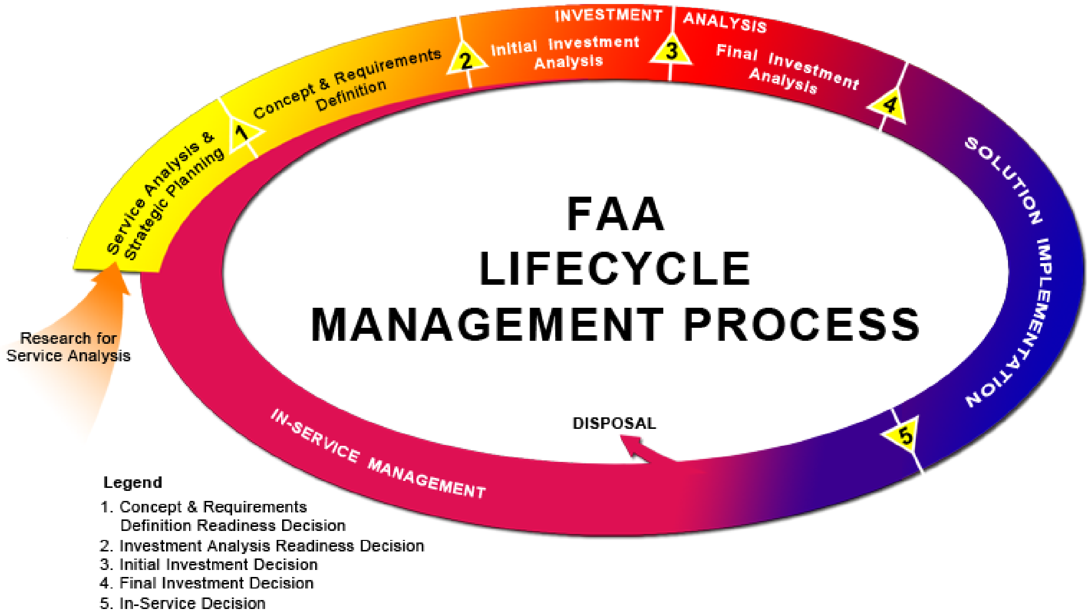

FAA LIFECYCLE MANAGEMENT PROCESS
INVESTMENT
ANALYSIS
Service Analysis & Strategic Planning
1
Concept & Requirements Definition
2
Initial Investment Analysis
3
Final Investment Analysis
4
SOLUTION IMPLEMENTATION
5
DISPOSAL
IN-SERVICE MANAGEMENT
Research for Service Analysis
Legend
1. Concept & Requirements Definition Readiness Decision
2. Investment Analysis Readiness Decision
3. Initial Investment Decision
4. Final Investment Decision
5. In-Service Decision

Figure C.1: FAA Lifecycle Management Process

2 Program Safety Requirements for a Concept and Requirements Definition Readiness Decision

2.1 Process Overview

Research and systems 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 determining whether to add a service shortfall or new operational concept to the National Airspace System (NAS) Concept of Operations and FAA Enterprise Architecture.

The Concept and Requirements Definition (CRD) Readiness Decision occurs when an enterprise architecture roadmap indicates action must be taken to address a critical mission opportunity or shortfall. It is based on completion of activities such as simulation, Functional Analysis (FA), and computer-human interface development to define requirements, develop operational concepts, and reduce safety risk before entering into Investment Analysis (IA).

With this decision, the Office of NextGen (ANG) NAS Systems Engineering Director verifies that the proposed service is a priority and time-critical investment opportunity, and that planning and resources for CRD are in place. The Director notifies the Joint Resources Council (JRC) of the decision to begin CRD.

2.2 Safety Outputs

2.2.1 Capability Safety Assessment

The portfolio manager is required to consider on a macro level whether the proposed operational capability might result in risk to the NAS. He or she must also consider and report any NAS safety issues that may influence or constrain the concept. The methodology for doing so may be a brainstorming session led by the Capability Safety Team's (CST's) ANG / Air Traffic Organization (ATO) Safety and Technical Training (AJI) co-leads to try to determine if the proposed operational capability would have a significant safety impact on the NAS. A more thorough approach uses FA to capture basic interface hazards that may be introduced into the NAS. The safety assessment for this phase should be in writing, must provide high-level safety considerations, and must state the results of this safety deliberation.

There may be enough data to develop a Capability Safety Assessment (CapSA) Report. CapSA Reports look at interactions among NAS components to identify hazards created on a capability level. Because linkages and complex distributed systems may not be obvious, FA can be an effective tool for such an assessment. The output may be similar to an Operational Safety Assessment (OSA) or a Functional Hazard Assessment, in that risk is not determined. Alternatively, the output may be similar to a Preliminary Hazard Analysis (PHA), employing a qualitative risk assessment. The initial CapSA Report is started in conjunction with the development of the capability's business case and must be periodically updated as necessary throughout the capability's lifecycle. Appendix B of the Safety Risk Management Guidance for System Acquisitions (SRMGSA) provides detailed guidance on how to prepare a CapSA Report.

2.2.2 Integrated System Safety Assessment

During the Service Analysis and Strategic Planning phase of the Acquisition Management System (AMS) process, and within the NAS Concept of Operations Change Development and Decomposition Process, an Integrated System Safety Assessment (ISSA) may be conducted to assess the feasibility of and identify potential safety critical issues associated with the idea or concept continuing through the AMS. An ISSA can involve Operational Sustainments, Operational Improvements, and increments; however, an ISSA is a smaller-scale assessment than a CapSA.

To effectively capture all possible interactions, an integration analysis must occur at several levels, as described in section 2.3 of the SRMGSA. The proposed integration analysis function is led by ANG and implemented by a cross-organizational Safety Collaboration Team of safety subject matter experts. The ISSA Report developed will provide an integrated framework for the safety assessment to ensure that individual Program Safety Teams (PSTs) do not overlook higher-level interaction hazards and to alert safety analysts to the possible invalidation of programmatic Safety Risk Management (SRM) results caused by subsequent changes to the NAS. The ISSA will provide actionable data to the appropriate stakeholders thereby providing them with the input necessary to effectively conduct a thorough safety assessment through each phase of the AMS. Thus, the output of the ISSA is a key input to the development of Program Safety Plans (PSPs) by the programs.

3 Program Safety Requirements for an Investment Analysis Readiness Decision

3.1 Process Overview

The Investment Analysis Readiness Decision (IARD) occurs at the end of the CRD phase. The IARD determines whether the Concept of Operations, preliminary requirements, enterprise architecture products and amendments, and preliminary alternatives are sufficiently defined to warrant entry into the IA phase. The decision is made within the context of all ongoing and planned investment activities to sustain and improve service delivery. It ensures proposals are consistent with overall corporate needs and planning.

If the concept under development requires that the proposed system, procedure, hardware, or software “go live” in the NAS for any demonstrations, flight tests, or prototypes, then SRM must be conducted. This safety assessment will typically use the PHA worksheet format. See the ATO Safety Management System (SMS) Manual for further details

CRD activities occur prior to the establishment of baseline requirements. An OSA that provides the system designers and management with a set of safety goals for design may be prepared. The OSA also provides an operational and environmental description, develops a Preliminary Hazard List (PHL) for the proposal, and assesses the potential severity of the hazards listed in the PHL.

In this phase, outputs from the CapSA Report or similar system-level analysis will provide inputs to the OSA. In addition, certain planning must occur prior to the IARD, such as developing an Investment Analysis Plan (IAP) that includes relevant safety information.

3.2 Safety Output

3.2.1 Program Safety Plan

The PSP is the Program Manager’s (PM’s) plan for the program’s safety process. The PSP is used to ensure compliance with provisions of the ATO SMS Manual. The PM 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 AJI and Service Unit policy and agreements made at the Safety Strategy Meeting (SSM). The ATO Chief Safety Engineer may require programs to identify additional features or text for inclusion.

A PSP must be developed and tailored specifically for each program asking for 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 CST/PST will further develop the PSP as the acquisition matures. At the IARD, the typical PSP should cover the following:

- Safety program scope and objectives
- Description of system/capability
- Safety organization
- Nominal safety program milestones
- General safety requirements
- Management of safety program
- Interfaces with other programs / capture teams

3.2.2 Operational Safety Assessment

The OSA is a tool based on the assessment of hazard severity. The OSA also establishes how safety requirements are to be allocated between air and ground components, and how this might influence performance and interoperability. 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 five or six weeks before the IARD date.

An OSA provides a disciplined method of objectively assessing the safety requirements of new NAS concepts and systems, typically for Communication, Navigation, and Surveillance and Air Traffic Management systems. The OSA identifies and assesses the hazards in a system, defines safety requirements, and builds a foundation for follow-on institutional safety analyses related to IA, Solution Implementation, In-Service Management (ISM), and Service Life Extension Programs.

OSA-identified severity codes are mapped to a pre-set level of probabilities, which establishes the necessary safety level required for controlling the hazard. This means that a hazard with a catastrophic severity would be mapped to a probability requirement more stringent than would a minor severity hazard. This process establishes the level needed for controlling the hazard at or below a medium risk level, which assists in establishing safety requirements for the concept or system design.

3.2.3 Software Development Assurance

Planning for development assurance needs to begin early in the AMS lifecycle so the Development Assurance Level (DAL), as defined in the SRMGSA, can be factored into the Business Case Analysis. Typically, this occurs prior to the IARD, while the OSA is being developed. The DAL is initially established from the OSA and is included in the preliminary Program Requirements Document (pPRD).

3.2.4 Preliminary Program Requirements Document

Preliminary program requirements specify how well the new capability must perform its intended functions. Safety is one of the key disciplines in the AMS and must be addressed. Safety requirements identified in the OSA that are also system requirements must be included as requirements in the pPRD.

3.2.5 Investment Analysis Plan

The IAP is a CRD phase requirement. It defines the program's scope, assumptions, alternatives, and organizational roles and responsibilities in IA. The IAP template is available on the FAST website. There is a section of the IAP that contains the requirement for reporting the results of safety assessments in the IAP as it is formulated and updated when the program goes through the AMS process. The IAP template is available on the FAST website.

4 Program Safety Requirements for the Initial Investment Decision

4.1 Process Overview

The Initial Investment Decision (IID) is the point at which the JRC approves or selects the best alternative that meets the required performance and offers the greatest value to the FAA and its customers. At this stage, the initial Program Requirements Document thoroughly defines the program's requirements and maintains requirements traceability. To support that decision, the Comparative Safety Assessment (CSA) is completed to inform the Program Management Organization (PMO) and JRC of the relative risk ratings of each alternative. In the AMS, the Portfolio Selection Criteria Guidance for the IID shows the role played by safety and is available on the FAST website.

4.2 Safety Outputs

4.2.1 Program Safety Plan

Prior to receiving an IID decision, the PSP must be updated with the latest information. At this phase of the acquisition lifecycle, there could be changes in the management and CST/PST as the program moves from ANG to ATO control. Also, the PM must plan to conduct the CSA, an essential analysis needed to receive an IID.

4.2.2 Comparative Safety Assessment

A CSA provides management with a listing of all of the hazards associated with a change, along with a risk assessment for each alternative hazard combination that is considered. 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 rank the options from a safety perspective for decision-making purposes. Other considerations for decision makers, such as cost, schedule, training, and other implications, are not within the scope of a CSA. Those considerations are discussed by the PMO in the IAP cost analysis and in similar Business Case reports.

The CSA is a risk assessment; it defines both severity and likelihood in terms of the initial and predicted residual risk of the solution. The likelihoods determined are for the worst credible outcome occurring. The CSA builds upon the OSA using the top-level FA from the OSA, but typically decomposing it by at least one more level in order to expand upon the PHL produced by the OSA. Each alternative is described in sufficient detail to ensure the audience can understand both the proposed solution and the hazards and risks developed. Per the AMS, alternatives selected and assessed are technical alternatives, not installation or procurement alternatives.

The expanded PHL is developed from the FA, at which point each hazard's risk is assessed in the context of the alternatives. For hazards related to human error, tools that specifically address human performance and reliability rates (including associated performance shaping) may be employed. (See the ATO SMS Manual for additional information.) After this is done, requirements and recommendations can be made based on the data in the CSA. A CSA should be written so that the decision-maker can clearly distinguish the relative safety merit of each alternative.

4.2.3 Software Development Assurance

The DAL, as defined by the SRMGSA, is validated in the CSA, which may differ between investment alternatives. The DAL for the alternatives is then included in the IAP and Implementation Strategy and Planning Document (ISPD) prior to the IID.

5 Program Safety Requirements for the Final Investment Decision

5.1 Process Overview

Systems safety has a twofold purpose leading up to the Final Investment Decision (FID): first, to develop early safety requirements that form the foundation of the safety and systems engineering efforts, and second, to provide objective safety data to aid acquisition management in their decisions. The early assessment saves time and money, allowing for informed, data-driven decisions.

The FID is the point at which the JRC approves the alternative that meets the required performance. This is called the preferred down-selection. To support that decision, a PHA is completed to inform the PMO and JRC of the risk ratings of that selection. The required work products of the Final IA must be verified and validated (according to the FAA AMS Verification and Validation (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 final Program Requirements Document (fPRD), final business case, and the final ISPD, all of which have safety embedded in them.

5.2 Safety Output

5.2.1 Program Safety Plan

At this point, the PSP must be once again updated and expanded, as it now forms the basis of the contractor's corresponding Systems Safety Program Plan (SSPP), if contractually required. The PSP supports the FID and is completed and approved prior to the JRC Secretariat's cut-off date for the FID.

The contractor's SSPP, when reviewed and approved, shows how and when the vendor or contractor intends to meet the specified PSP requirements. The review and approval authority for the SSPP is the ATO PMO, with concurrence from the ATO Chief Safety Engineer. The SSPP details the following:

- Contractor's program scope
- Safety organization
- Program milestones
- Requirements and criteria
- Hazard analyses
- Safety data
- Verification of safety requirements
- Auditing and monitoring program
- Post-Implementation Review (PIR) plans
- Training
- Accident and incident reporting
- Interfaces

The Data Item Description (DID) for an SSPP, located in appendix D of the SRMGSA, outlines the contents to be included in the SSPP.

The typical PSP prior to the FID covers the following:

- Program scope and objectives
- Safety organization
- Safety program milestones
- General safety requirements and criteria
- Hazard analyses to be performed
- Hazard tracking system processes to be used
- Safety data to be collected

- Safety requirements management, including how to manage the Safety Requirements Verification Table (SRVT)
- Safety assessments and reports for changes to program, design, and engineering
- Safety training required
- Safety interfaces with design engineering, contractors, management, and other specialty engineering groups
- Safety Assessment Review Plan (i.e., the type of safety assessment program to be used and scheduled for accomplishing safety V&V)
- PSP management of cost and schedules
- Interfaces with other program and integrated safety plans

5.2.2 Preliminary Hazard Analysis

The PHA is a common hazard identification and analysis tool used in nearly all SMS applications. Its broad scope is an excellent guide 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. In addition to the historical experiences used for the PHL, information about technologies, materials, and architectural features such as redundancy and human-system integration are available as sources of the PHA.

The PHA can be conducted as an output of the OSA, CSA, FA, and/or the bow-tie model. It is important to note that the OSA and CSA may not have been performed if the ATO Chief Safety Engineer waived the requirement to perform those assessments. Although an FA or a bow-tie model is not required, they are both highly recommended, as they can assist in the hazard identification process and subsequent portions of the analysis. A human reliability analysis or assessment (the expansion of the PHL to include risks, hazards, credible effects, and mitigations to manage the risk) may also be conducted.

The PHA is conducted after the alternatives are evaluated and a single alternative is selected as the best option. This means it is conducted after the CSA and before the FID. The PHA subset of the Safety Risk Management Document (SRMD) is completed and approved prior to the JRC Secretariat's cut-off date for the FID. The DID for a PHA, located in appendix D of the SRMGSA, outlines the contents to be included in the PHA.

5.2.3 Final Program Requirements Document

The fPRD contains all new and existing systems safety requirements accepted by the program. The mitigations identified in the SRMD that are allocated to the program must show up as requirements in the fPRD. These requirements must be uniquely identified and be able to be parsed into the SRVT. If all the identified safety requirements in the fPRD are eventually verified, the program will attain its predicted residual risk. If not, the resultant risk rating may be as high as the initial risk ratings determined in the PHA.

5.2.4 Implementation Strategy and Planning Document

The ISPD provides the investment decision authority with a summarized characterization of the plans for the Solution Implementation of the proposed investment. It conveys the most critical, relevant, and meaningful information to support JRC decision-making. The IID requires an initial ISPD covering specific sections identified in the ISPD template. An FID requires a complete ISPD. After the FID, the ISPD can only be modified if the program returns to the JRC for a change to the investment decision.

Within the ATO, the ISPD is approved by both the vice president of the organization that will execute the program and by the Chief Operating Officer. Certain sections of the ISPD are reviewed and approved by specific executives, including the Vice President of AJI. Final signed approval of the ISPD by all members of the JRC is concurrent with the investment decision. There is a section of the ISPD specific to the SMS. The ISPD template is available on the FAST website.

5.2.5 Software Development Assurance

The final DAL, as defined in the SRMGSA, is determined from the PHA. This final DAL is included in the fPRD and PSP. Any changes to DAL are included in the final versions of the Business Case Analysis and ISPD prior to the FID.

6 Program Safety Requirements for an In-Service Decision

6.1 Process Overview

The In-Service Decision (ISD) authorizes deployment of a solution into the operational environment, and occurs after demonstration of Initial Operating Capability (IOC) at the key site. The ISD establishes the foundation for the declaration of operational readiness at the key site, and IOC at subsequent sites. An approved SRMD is required at IOC, and must then be updated prior to the ISD to reflect national deployment. Prior to the ISD, all of the safety-related In-Service Review (ISR) checklist items must be closed or have an approved Action Plan. The ATO Chief Safety Engineer must concur with the closure of the ISR checklist items and any related Action Plans. The Director of Policy and Performance approves the Action Plan as the Closing Authority, and he or she concurs with the closure of the Action Plan. Statuses of ISD Action Plans are reported to the ISD Secretariat and tracked to closure.

The full suite of safety analyses required by the ATO and the SSM, all of which are listed in the PSP and SSPP, must be done prior to the ISD. Typical safety assessments, usually performed by the prime vendor or its sub-contractor, include those listed in the Safety Output section below.

6.2 Safety Output

6.2.1 Program Safety Plan

Prior to ISD, the PSP must be expanded to include any safety planning required to support the PIR.

6.2.2 Sub-System Hazard Analysis

A Sub-System Hazard Analysis (SSHA) is a safety risk assessment of a system’s sub-systems/components conducted by the system developer at a deeper level than is provided in a PHA. In cases where system development is performed by the vendor, the SSHA is typically assigned per the Statement of Work. The SSHA uses the same worksheet as the PHA and is performed early in the lifecycle of a system, providing valued inputs to the development of requirements in the early phases of system development. It is an analysis type that examines each sub-system or component (including the human component); identifies hazards associated with normal and abnormal operations; and is intended to determine 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 systems safety requirements and to assist in preparing performance and design specifications. In addition, the SSHA establishes the framework for the performance of follow-on hazard analyses.

The SSHA is the central part of any systems safety program. It provides detailed analysis that identifies hazards and recommends solutions. The design details are known and the analyses cover all details that are necessary to identify all possible safety risks.

Most SSHAs are documented in the matrix format, though some use fault trees or other forms of logic diagrams. Fault trees 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.

SSHAs are more detailed than the PHA, and are intended to show that the sub-system design meets the safety requirements in the sub-system specifications. If hazards are not identified and corrected during the design process, they might not be identified and corrected later when the sub-system designs are frozen and the cost of making a change is significantly increased.

The DID for an SSHA, located in appendix D of the SRMGSA, outlines the contents to be included in the SSHA.

6.2.3 System Hazard Analysis

The System Hazard Analysis (SHA) analyzes the whole system and the internal and external system interfaces. Its general purpose is to perform a detailed safety risk assessment of a system's interfaces with other systems and the interfaces between the sub-systems that compose the system being studied.

The SHA is conducted by the system developer. In cases when system development is performed by the vendor, the SHA is typically assigned per the Statement of Work. The SHA uses the same worksheet as the PHA, and is performed early in the Solution Implementation phase of the lifecycle of a system, providing important input to the development of requirements in the early phases of system development. The SHA aids in the early determination of risk and the need for additional safety requirements for system hazards. The output of the SHA may be used to develop additional systems safety requirements and to assist in preparing performance and design specifications. In addition, the SHA is a basic hazard analysis that establishes the framework for follow-on hazard analyses that may be performed.

The SHA should begin as the system design matures, at the preliminary design review or the facilities concept design review milestone. It should be updated until the design is complete. The SHA is used to identify new requirements and support the V&V of existing requirements.

For the most part, the description of the SSHA also applies to the SHA.

The specific uses of the SHA are to:

- Verify system compliance with safety requirements in the system specification;
- Identify previously unidentified hazards associated with the system interfaces, system functional faults, and system operation in the specified environment;

- Assess the safety risk of the total system design;
- Consider human factors, system/functional failures, and functional relationships between sub-systems comprising the system (including software);
- Identify and verify existing controls;
- Initiate and/or update the SRVT;
- Recommend and validate additional mitigations or controls; and
- Develop processes to control and track hazards.

The DID for an SHA, located in appendix D of the SRMGSA, outlines the contents to be included in the SHA.

6.2.4 Operating and Support Hazard Analysis

The general purpose of the Operating and Support Hazard Analysis (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 uses the same worksheet as the PHA and 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 controlling procedural hazards instead of only those hazards created by design. Additionally, the O&SHA should 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 test and evaluation. As a result, the O&SHA is typically the last formal analysis to be completed, usually mid-way through the Solution Implementation 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). This is critical; design and construction of support facilities must begin far before the system is ready for fielding, and all special safety features must be identified early on, or the costs to modify the facilities may force PMs and users to accept unnecessary risks.

It is important to ensure that the analysis considers not only the normal operation of the system, but also abnormal, emergency, or degraded operation; system installation; maintenance; servicing; storage; evaluation of training; and other operations. Misuse must also be considered. In other words, if anyone will be doing anything with the system, planned or unplanned, the O&SHA should cover it.

The DID for an O&SHA, located in appendix D of the SRMGSA, outlines the contents to be included in the O&SHA.

6.2.5 System Safety Assessment Report

The general purpose of a System Safety Assessment Report (SSAR) is to conduct and document a comprehensive evaluation of the safety risk being assumed before the program is deployed into the NAS. This means that the SSAR summarizes the safety analyses and assessments previously conducted on the program. The SSAR is a continuous, closed-loop process containing the SRVT. The SRVT contains all of the safety requirements identified with the origin of the requirement (e.g., OSA, CSA, PHA, SHA), including V&V. At the ISD or IOC, all safety requirements must undergo V&V by the ATO PMO. Objective evidence of V&V closed status may be reviewed by the ATO Chief Safety Engineer upon request.

Per the ATO SMS Manual and the FAA NAS Systems Engineering Manual (SEM), validation is the process of proving that the right product is being built (i.e., that the requirements are unambiguous, correct, complete, and verifiable). Verification is the process that ensures that the requirements have been met by the design solution and that the product is ready to be deployed in the operational environment for which it was originally intended.

The report provides an overall assessment of the safety risk associated with the product. It is crucial that this assessment report be developed as an encapsulation of all the analyses performed. For Independent Operational Assessment (IOA)−designated systems, it must be updated to reflect IOA results as appropriate. Safety hazards documented during IOA should be evaluated by the PST to determine if there is impact on prior safety analyses, determine if additional analysis is needed, and then develop appropriate mitigations and monitoring for the IOA safety hazards. The SSAR contains a summary of the analyses performed and their results, the tests conducted and their results, and the compliance assessment. The SSAR must include:

- The safety criteria and methodology used to classify and rank hazards, including any assumptions made from which the criteria and methodologies were derived;
- The results of the analyses, demonstrations, assessments, and testing conducted;
- The hazards that have an identified residual risk and the assessment of that risk;
- The list of hazards and the specific safety recommendations or precautions required to reduce their safety risk; and
- A discussion of the management and engineering decisions affecting the residual risk at a system level.

The final section of the SSAR should be a statement by the PMO describing the overall risk associated with the system and the PMO’s acceptance of that risk.

The DID for an SSAR, located in appendix D of the SRMGSA, outlines the contents to be included in the SSAR.

6.2.5.1 How to Use the SSAR

An SSAR must be conducted prior to any ISD or IOC decision point. Conducting the SSAR is an ISR requirement.

The specific uses of the SSAR are to:

- Summarize the results of the program’s SRM efforts;
- Identify all safety features of hardware, software, interfaces, and system design;
- Identify hazards related to procedures, human factors, hardware, and software identified in the program to date;

- Update the SRVT to show the V&V status of each safety requirement and the hazards to which those requirements are applied; and
- Assess readiness based on safety risk when proceeding with test or operation.

All hazards must be included in a monitoring plan. This must be approved by the ATO Chief Safety Engineer as part of the SSAR. In the event that the SSAR reveals some requirements not yet verified, the risk may need to be reassessed for accuracy. The PST will submit the results of the SSAR to the ATO Chief Safety Engineer.

As previously mentioned, the statuses of mitigations are shown in the SRVT. Before IOC, AJI and the ATO PMO work together to determine if the listed safety requirements have been met to a point where IOC can be declared. This is done on a case-by-case basis. After IOC and before an ISD is declared, the PMO may conduct an Operational Suitability Demonstration, and AJI may conduct an Independent Assessment. This may lead to the identification of additional safety requirements, and the SSAR/SRVT will have to be updated.

6.2.5.2 Types of Safety Reviews

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

- **Periodic Review**
  These are reviews done throughout the life of a program. They evaluate the status of hazards based on the verification of controls and requirements, and help in monitoring the effectiveness of the controls.

- **Phased Review**
  These are reviews conducted for defined portions of the implementation of solutions into the NAS. Phased reviews apply to a single JRC decision, which involves implementing a solution in steps or phases. The program itself does not need to use the term “phased” in its title. As long as the implementation is incremental or in steps, each increment or step will have safety reviews. The reviews evaluate the status of hazards based on the verification of mitigating requirements for that particular phase.

- **Final Implementation Review**
  These are reviews conducted for a program’s ISD and IOC. The reviews evaluate the status of hazards based on the verification of the program’s requirements.

6.2.6 Safety Requirements Verification Table

The SRVT is an evolving list of safety requirements that starts with the first safety assessment. Safety requirements are controls written in requirements language and used to control hazards. Changes to safety requirements must be reported to the program office and to the ATO Chief Safety Engineer.

The SRVT contains the following information:

- A list of requirements identified in any safety assessment for a given program (e.g., OSA, CSA, PHA, SHA/SSHA, O&SHA),
- V&V information, and
- The level of risk controlled by the requirement.

6.2.6.1 Using the SRVT

The SRVT is used to accomplish the V&V process for safety requirements. The ATO PMO must assure all safety requirements are captured within the SRVT.

The SRVT is intended to provide a continuing list and status of safety requirements that result from the SRM process. The requirements that are contained in this list must meet the standards detailed in the FAA NAS SEM.

6.2.7 Software Development Assurance

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

6.2.8 ISR Checklist

The ISR checklist is specific to systems safety and must be completed in support of the ISD. By reviewing the checklist early in a program's AMS lifecycle, the PMO will better understand the steps that must be completed. As programs approach ISD, the AJI Safety Case Lead, on behalf of the ATO PMO, will coordinate with the AJI Safety Engineering Team Manager to ensure that the systems safety management portion of the checklist (section 14) has been completed. The ISR checklist may be downloaded from the ISD page of the FAA employee website, located at https://employees.faa.gov/org/linebusiness/ato/safety/isd/.

7 Program Safety Requirements for In-Service Management

7.1 Process Overview

7.1.1 Monitoring Mitigations and Tracking Hazards

See the ATO SMS Manual for detailed guidance on risk monitoring and tracking.

7.1.2 Post-Implementation Review Safety Considerations

A PIR is an evaluation tool used to assess the results of an investment program against baseline expectations 6 to 24 months after it goes into operational service. Its main objective is to assess an investment program, determining if it is achieving expected performance and benefit targets, if it is meeting the service needs of customers, and if the original business case is still valid. The PIR process is governed by section 4.15.1 of the AMS.

A PIR Strategy is developed during the AMS lifecycle during the Final IA. It 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 upon their assigned acquisition category. SMS considerations for inclusion in the PIR Strategy are discussed during an SSM held with the ATO Chief Safety Engineer, PIR Quality Officer, and the PMO.

A PIR plan is developed prior to ISD during the AMS lifecycle by the PIR Team[1] for the investment program under review. It is a detailed expansion and refinement of the PIR

[1] The PIR is organized and managed by the PIR Quality Officer in Acquisition Policy and Oversight / Acquisition and Contracting / Office of Finance and Management.

Strategy, defining expected outcomes, planned activities, and resources necessary to complete the review. SRM input to the plan should be finalized after the SSAR is completed and approved. The ATO Chief Safety Engineer reviews the safety input to the PIR plan and provides concurrence or recommendations to the PIR Team Leader and PIR Quality Officer.

A PIR report is prepared by the PIR Team[2] after the review is completed. The ATO Chief Safety Engineer reviews the report's safety findings and recommendations and provides concurrence or recommendations to the PIR Quality Officer.

After the PIR report is complete, a plan of action and milestones (with completion dates) are developed to address the report's recommendations. These recommendations support the ISM phase during the AMS lifecycle and are reported to the investment decision authority, Vice President or equivalent, and key stakeholders, including AJI.

See the FAST website for information on how to conduct a PIR and report results, including those specific to SRM. Refer to the ATO SMS Manual for additional details of assessments and evaluation.

[2] The ATO Chief Safety Engineer should participate as a member of the PIR Team.

Appendix D

Data Item Descriptions

DATA ITEM DESCRIPTION

Title: Preliminary Hazard Analysis

Number: AJI-DID-PHA-001	**Approval Date:** TBD
AMSC Number: N/A	**Limitation:** N/A
DTIC Applicable: No	**GIDEP Applicable:** No

Office of Primary Responsibility: Air Traffic Organization Safety and Technical Training, Integrated Safety Policy Team
Applicable Forms: N/A

Use/relationship:

The Preliminary Hazard Analysis (PHA) is the initial hazard identification effort conducted during the programming and requirements development phase of an acquisition. The PHA focuses on the details of the early system design (including their implications for human reliability) and is primarily used to perform an initial risk assessment to develop early safety-related requirements and specifications. The PHA is used to both identify new requirements and to support the verification and validation of existing requirements.

The PHA, since it is performed early in the lifecycle of a system, provides important inputs to the development of system requirements. In the case of an operational system, the PHA aids in the early determination of risk and the need for additional safety requirements to mitigate operational risks. The output of the PHA will be used to develop systems safety requirements and to assist in preparing performance and design specifications. In addition, the PHA establishes the framework for follow-on hazard analyses that may need to be performed.

This Data Item Description (DID) contains the format, content, and preparation instructions for the PHA.

This DID supersedes FAA-DI-SAFT-101.

Requirements:

1. Reference Documents:
   - The Air Traffic Organization (ATO) Safety Management System (SMS) Manual
   - The Safety Risk Management Guidance for System Acquisitions (SRMGSA)

2. Format: The report must be prepared as an SRMD using the guidelines contained in the ATO SMS Manual.

3. Content: The PHA must be written in accordance with the requirements of the ATO SMS Manual and the SRMGSA. The description of each identified hazard must contain, at a minimum, the information prescribed in paragraphs 3.1 through 3.16.

   3.1. Hazard Name: Alpha-numeric identifiers will be used to track hazards through the verification and validation process. Unique identifiers must be created and marked for individual hazards, or sequences created for clustered hazards or subsets.

3.2. Hazard Description: A complete statement describing the hazard. The ATO SMS Manual defines a hazard as, "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." A hazard is a condition that is a prerequisite to an accident or incident.

3.3. Cause(s): Events that result in a hazard or failure. Causes can occur by themselves or in combinations. They may include, but are not limited to, human error, latent failure, active failure, design flaw, component failure, and software error.

3.4. System State: An expression of the various conditions, characterized by quantities or qualities, in which a system can exist. System state is described for each individual hazard associated with the system (e.g., adverse weather and lighting conditions, such as day, dusk, and night). The system state will also include the activity under which the harm may occur (e.g., storage; shipping; installation; testing; maintenance; replacement; decommissioning; or phase of flight, such as en route or taxiing). Any given hazard may have a different risk level in each possible system state. Hazard assessment must consider all possibilities while allowing for all system states. It is important to capture different system states in a hazard analysis when the end results lead to the application of different mitigations. System state must be defined in accordance with the ATO SMS Manual.

3.5. Existing Controls: The existing safeguards, safety features, protective devices, warnings, training, and procedures that control or eliminate risk. An existing safety control is a requirement that exists currently in the Federal Aviation Administration (e.g., controls that were previously defined in prior analyses) that is validated or verified to mitigate or manage the risk of a hazard's effect or occurrence.

3.6. Existing Control Justification / Supporting Data: The explanation of how existing controls were validated and verified.

3.7. Effects: The real or credible harmful outcome(s) that can be expected if the hazard occurs in the defined system state.

3.8. Severity: The measure of how bad the results of an event are predicted to be. Severity is determined by the worst credible outcome. Less severe effects may be considered analytically in addition to this, but at a minimum, the most severe effects are to be considered. Do not consider likelihood when determining severity; determination of severity is independent of likelihood. Determine the severity classifications from the ATO SMS Manual.

3.9. Severity Rationale: The explanation of how the severity was determined.

3.10. Likelihood: Likelihood is an expression of how often an event is expected to occur. Severity must be considered in the determination of likelihood. Likelihood is determined by how often the resulting harm can be expected to occur at the worst credible severity. When determining likelihood, the worst credible system

states will usually determine the worst credible severity. Determine the likelihood classifications from the ATO SMS Manual.

3.11. Likelihood Rationale: The explanation of how likelihood was determined.

3.12. Initial Risk: The composite of the severity and likelihood of a hazard considering only verified controls and documented assumptions for a given system state. It describes the risk at the preliminary or beginning stage of a proposed change, program, or assessment. Initial risk is determined by factoring both verified controls and assumptions into the system state. When assumptions are made, they must be documented as recommended controls. Once the initial risk is established, it is not changed.

3.13. Recommended Safety Requirements: The suggested mitigations or controls that have the potential to mitigate a hazard or risk but have not yet been validated or verified as part of the system or its requirements.

3.14. Organization Responsible for Implementing Safety Requirements: The organization's name and the point of contact's name and number.

3.15. Predicted Residual Risk: The term used until the safety analysis is complete and all safety requirements have been verified. Predicted residual risk is based on the assumption that all safety requirements will be validated and verified.

3.16. Safety Performance Targets: The measurable goals that will be used to verify the predicted residual risk of a hazard.

DATA ITEM DESCRIPTION

Title: Systems Safety Program Plan

Number: AJI-DID-SSPP-001	**Approval Date:** TBD
AMSC Number: N/A	**Limitation:** N/A
DTIC Applicable: No	**GIDEP Applicable:** No

Office of Primary Responsibility: Air Traffic Organization Safety and Technical Training, Integrated Safety Policy Team
Applicable Forms: N/A

Use/relationship:

In the Systems Safety Program Plan (SSPP), the contractor must detail the systems safety program scope, safety organization, program milestones, safety requirements and criteria, hazard analyses to be conducted, safety data to be collected, safety verification approach, safety program audit process, accident/incident reporting system, and the organization's functional interfaces.

The SSPP must include details of those methods the contractor will use to implement each systems safety task called for in the government-provided Program Safety Plan, the Statement of Work, and those safety-related documents listed in the contract for compliance. Examples of safety-related documents include Occupational Safety and Health Administration regulations; DO-264, *Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications*; DO-278A, *Guidelines for Communication, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance*; DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*; and other national standards, such as the National Fire Protection Association. The SSPP will list all requirements, activities, and the appropriate related tasks required to satisfy the systems safety program objectives. A complete breakdown of systems safety tasks, subtasks, and resource allocations of each program element through the term of the contract also needs to be included. When designated in the contract, a baseline SSPP will be required at the beginning of the first contractual phase (e.g., Demonstration and Validation or Full-Scale Development) and updated at the beginning of each subsequent phase (e.g., Production) to describe the tasks and responsibilities of the follow-on phase.

This Data Item Description (DID) contains the format, content, and preparation instructions for the SSPP.

This DID supersedes FAA-DI-SAFT-102.

Requirements:

1. Reference Documents:
    - The Air Traffic Organization (ATO) Safety Management System Manual
    - The Safety Risk Management Guidance for System Acquisitions (SRMGSA)
    - The National Airspace System (NAS) Systems Engineering Manual (SEM)

2. Format: The SSPP format must be "contractor selected." Unless the effective presentation would be degraded, the initially selected format must be used for all subsequent submissions.

3. Content: The SSPP must contain the items prescribed in paragraphs 3.1 through 3.12.

   3.1. Program Scope: The plan must include a systematic, detailed description of the scope and magnitude of the overall systems safety program and the tasks to implement it. This includes a breakdown of the project by organizational components, 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 effectively implement the contractual task.

   3.2. Systems Safety Organization: The plan must detail the contractor's systems safety organization by including the following information:

      - The contractor's systems safety organization or function as it relates to the contractor's program organization and to the corresponding government entities (including the role of any subcontractors),
      - The responsibility and authority of all contractor personnel involved with the contractor's safety program,
      - The staffing plan of the contractor's systems safety organization for the duration of the contract,
      - The procedures by which the contractor will integrate and coordinate the systems safety efforts,
      - The process by which contractor management decisions will be made,
      - Who or which organization does the work identified in paragraph 3.1,
      - The internal organizations that approve the work identified in paragraph 3.1,
      - The internal organizations that receive the work identified in paragraph 3.1, and
      - How the contractor will interface with the government's Program Safety Team (PST) and the ATO Chief Safety Engineer.

   3.3. Program Milestones: The plan must briefly describe the safety tasks and products that the contractor will conduct and produce. This will include a program schedule (e.g., Gantt chart) of the safety tasks, including start and completion dates, reports, design reviews, and estimated staff loading.

   3.4. Work Products: The plan must describe work products that will be produced (e.g., Preliminary Hazard Analysis, Sub-system Hazard Analysis, System Hazard Analysis, Operating and Support Hazard Analysis).

   3.5. Requirements and Criteria: The plan must describe the safety performance requirements (e.g., qualitative values, accident risk values, or standardized values); safety design requirements as established by the PST; and required documentation, including descriptions of risk assessment procedures (types of analyses to be performed) and safety precedence (the method of controlling specific unacceptable hazards), in accordance with the section 4.3 of the NAS SEM.

3.6. Hazard Analyses: The plan must describe the specific hazard analyses to be performed during the program. The analysis techniques and formats should be qualitative or quantitative to identify risks, the hazards and effects of these risks, hazard elimination or risk reduction requirements, and the way these requirements are to be met, in accordance with the SRMGSA.

3.7. Safety Data: The plan must provide a list of systems safety tasks, a contract data requirements list having safety significance, and the requirement for a contractor systems safety data file containing all relevant safety data. The data in the file is not a deliverable, but is to be made available for the government's review upon formal request.

3.8. Safety Verification: The plan must describe the safety verification test and/or assessment program to be used to demonstrate the safety verification process, in accordance with section 4.12 of the NAS SEM.

3.9. Audit Program: The plan must provide a description of the techniques and procedures to be used to verify that the requirements of the systems safety process are being met.

3.10. Training: Once the hazards related to training have been identified, the plan must describe the procedures to be applied to training operator, maintenance, and test personnel.

3.11. Accident/Incident Reporting: The plan must describe the details and timing of the notification process for the program and the method of ensuring that the incidents/accidents during system development are translated to potential operational hazards. Once the hazards are identified, they must be incorporated into a hazard tracking system.

3.12. Interfaces: The plan must describe the requirements used to coordinate all the different interfaces of the contract, in accordance with section 4.7 of the NAS SEM.

DATA ITEM DESCRIPTION

Title: Sub-System Hazard Analysis
Number: AJI-DID-SSHA-001 **Approval Date:** TBD
AMSC Number: N/A **Limitation:** N/A
DTIC Applicable: No **GIDEP Applicable:** No
Office of Primary Responsibility: Air Traffic Organization Safety and Technical Training, Integrated Safety Policy Team
Applicable Forms: N/A

Use/relationship:

The general purpose of the Sub-System Hazard Analysis (SSHA) is to perform a safety risk assessment of a system's sub-systems/components at a greater level than that provided in a Preliminary Hazard Analysis. The contractor must perform an SSHA if a system under development contains sub-systems or components that, when integrated, function together in a system. The contractor must examine each sub-system or component (including the human component), identify hazards associated with normal and abnormal operations, and determine how operation or failure of components (or any other anomaly) adversely affects the overall safety of the system. The SSHA should identify existing and recommended actions using the systems safety precedence to determine how to eliminate or reduce the risk of identified hazards.

The SSHA is performed in the early stages of Solution Implementation. In the case of an operational system, it aids in the early determination of risk and the need for additional safety requirements to mitigate operational hazards. The output of the SSHA will be used to develop systems safety requirements, to assist in preparing performance and design specifications, and to support the verification and validation of existing requirements. In addition, the SSHA will be a basic hazard analysis that establishes the framework for follow-on hazard analyses that may need to be performed.

This Data Item Description (DID) contains the format, content, and preparation instructions for the SSHA.

This DID supersedes FAA-DI-SAFT-103.

Requirements:

1. Reference Documents:
    - The Air Traffic Organization (ATO) Safety Management System (SMS) Manual
    - The Safety Risk Management Guidance for System Acquisitions (SRMGSA)

2. Format: The report must be prepared as a Safety Risk Management Document using the guidelines contained in the ATO SMS Manual.

3. Content: The SSHA must be written in accordance with the requirements of the ATO SMS Manual and the SRMGSA. The description of each identified hazard must contain, at a minimum, the information prescribed in paragraphs 3.1 through 3.16.

3.1. Hazard Name: Alpha-numeric identifiers will be used to track hazards through the verification and validation process. Unique identifiers must be created and marked for individual hazards, or sequences created for clustered hazards or subsets.

3.2. Hazard Description: A complete statement describing the hazard. The ATO SMS Manual defines a hazard as, "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." A hazard is a condition that is a prerequisite to an accident or incident.

3.3. Cause(s): Events that result in a hazard or failure. Causes can occur by themselves or in combinations. They may include, but are not limited to, human error, latent failure, active failure, design flaw, component failure, and software error.

3.4. System State: An expression of the various conditions, characterized by quantities or qualities, in which a system can exist. System state is described for each individual hazard associated with the system (e.g., adverse weather and lighting conditions, such as day, dusk, and night). The system state will also include the activity under which the harm may occur (e.g., storage; shipping; installation; testing; maintenance; replacement; decommissioning; or phase of flight, such as en route or taxiing). Any given hazard may have a different risk level in each possible system state. Hazard assessment must consider all possibilities while allowing for all system states. In a hazard analysis, it is important to capture different system states when the end results lead to the application of different mitigations. System state must be defined in accordance with the ATO SMS Manual.

3.5. Existing Controls: The existing safeguards, safety features, protective devices, warnings, training, and procedures that control or eliminate risk. An existing safety control is a requirement that exists currently in the Federal Aviation Administration (e.g., controls that were previously defined in prior analyses) that is validated or verified to mitigate or manage the risk of a hazard's effect or occurrence.

3.6. Existing Control Justification / Supporting Data: The explanation of how existing controls were validated and verified.

3.7. Effects: The real or credible harmful outcome(s) that can be expected if the hazard occurs in the defined system state.

3.8. Severity: The measure of how bad the results of an event are predicted to be. Severity is determined by the worst credible outcome. Less severe effects may be considered analytically in addition to this, but at a minimum, the most severe effects are to be considered. Do not consider likelihood when determining severity; determination of severity is independent of likelihood. Determine the severity classifications from the ATO SMS Manual.

3.9. Severity Rationale: The explanation of how the severity was determined.

3.10. Likelihood: Likelihood is an expression of how often an event is expected to occur. Severity must be considered in the determination of likelihood. Likelihood is determined by how often the resulting harm can be expected to occur at the worst credible severity. When determining likelihood, the worst credible system states will usually determine the worst credible severity. Determine the likelihood classifications from the ATO SMS Manual.

3.11. Likelihood Rationale: The explanation of how likelihood was determined.

3.12. Initial Risk: The composite of the severity and likelihood of a hazard considering only verified controls and documented assumptions for a given system state. It describes the risk at the preliminary or beginning stage of a proposed change, program, or assessment. Initial risk is determined by factoring both verified controls and assumptions into the system state. When assumptions are made, they must be documented as recommended controls. Once the initial risk is established, it is not changed.

3.13. Recommended Safety Requirements: The suggested mitigations or controls that have the potential to mitigate a hazard or risk but have not yet been validated or verified as part of the system or its requirements.

3.14. Organization Responsible for Implementing Safety Requirements: The organization’s name and the point of contact’s name and number.

3.15. Predicted Residual Risk: The term used until the safety analysis is complete and all safety requirements have been verified. Predicted residual risk is based on the assumption that all safety requirements will be validated and verified.

3.16. Safety Performance Targets: The measurable goals that will be used to verify the predicted residual risk of a hazard.

DATA ITEM DESCRIPTION

Title: System Hazard Analysis
Number: AJI-DID-SHA-001 **Approval Date:** TBD
AMSC Number: N/A **Limitation:** N/A
DTIC Applicable: No **GIDEP Applicable:** No
Office of Primary Responsibility: Air Traffic Organization Safety and Technical Training, Integrated Safety Policy Team
Applicable Forms: N/A

Use/relationship:

The System Hazard Analysis (SHA) is a safety risk assessment of a system that analyzes the interfaces of a system with other systems, as well as the interfaces between the sub-systems of the system under study. The contractor-performed Sub-System Hazard Analysis serves as input to the SHA. The SHA should begin as the system design matures, at the preliminary design review or the facilities concept design review milestone, and should be updated until the design is complete. The SHA is used to both identify new requirements and to support the verification and validation of existing requirements.

The SHA is performed early in the lifecycle of a system, providing important inputs to the development of requirements in the early phases of system development. In the case of an operational system, it aids in the early determination of risk and the need for additional safety requirements for operational hazards. The output of the SHA will be used to develop systems safety requirements and to assist in preparing performance and design specifications. In addition, the SHA, as a basic hazard analysis, establishes the framework for follow-on hazard analyses that may be performed.

This Data Item Description (DID) contains the format, content, and preparation instructions for the SHA.

This DID supersedes FAA-DI-SAFT-104.

Requirements:

1. Reference Documents:
    - The Air Traffic Organization (ATO) Safety Management System (SMS) Manual
    - The Safety Risk Management Guidance for System Acquisitions (SRMGSA)

2. Format: The report must be prepared as a Safety Risk Management Document using the guidelines contained in the ATO SMS Manual.

3. Content: The SHA must be written in accordance with the requirements of the ATO SMS Manual and the SRMGSA. The description of each identified hazard must contain, at a minimum, the information prescribed in paragraphs 3.1 through 3.16.

    3.1. Hazard Name: Alpha-numeric identifiers will be used to track hazards through the verification and validation process. Unique identifiers must be created and marked for individual hazards, or sequences created for clustered hazards or subsets.

3.2. Hazard Description: A complete statement describing the hazard. The ATO SMS Manual defines a hazard as, "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." A hazard is a condition that is a prerequisite to an accident or incident.

3.3. Cause(s): Events that result in a hazard or failure. Causes can occur by themselves or in combinations. They may include, but are not limited to, human error, latent failure, active failure, design flaw, component failure, and software error.

3.4. System State: An expression of the various conditions, characterized by quantities or qualities, in which a system can exist. System state is described for each individual hazard associated with the system (e.g., adverse weather and lighting conditions, such as day, dusk, and night). The system state will also include the activity under which the harm may occur (e.g., storage, shipping, installation, testing, maintenance, replacement, decommissioning, or phase of flight, such as en route or taxiing). Any given hazard may have a different risk level in each possible system state. Hazard assessment must consider all possibilities while allowing for all system states. In a hazard analysis, it is important to capture different system states when the end results lead to the application of different mitigations. System state must be defined in accordance with the ATO SMS Manual.

3.5. Existing Controls: The existing safeguards, safety features, protective devices, warnings, training, and procedures that control or eliminate risk. An existing safety control is a requirement that exists currently in the Federal Aviation Administration (e.g., controls that were previously defined in prior analyses) that is validated or verified to mitigate or manage the risk of a hazard's effect or occurrence.

3.6. Existing Control Justification / Supporting Data: The explanation of how existing controls were validated and verified.

3.7. Effects: The real or credible harmful outcome(s) that can be expected if the hazard occurs in the defined system state.

3.8. Severity: The measure of how bad the results of an event are predicted to be. Severity is determined by the worst credible outcome. Less severe effects may be considered analytically in addition to this, but at a minimum, the most severe effects are to be considered. Do not consider likelihood when determining severity; determination of severity is independent of likelihood. Determine the severity classifications from the ATO SMS Manual.

3.9. Severity Rationale: The explanation of how the severity was determined.

3.10. Likelihood: Likelihood is an expression of how often an event is expected to occur. Severity must be considered in the determination of likelihood. Likelihood is determined by how often the resulting harm can be expected to occur at the worst credible severity. When determining likelihood, the worst credible system

states will usually determine the worst credible severity. Determine the likelihood classifications from the ATO SMS Manual.

3.11. Likelihood Rationale: The explanation of how likelihood was determined.

3.12. Initial Risk: The composite of the severity and likelihood of a hazard considering only verified controls and documented assumptions for a given system state. It describes the risk at the preliminary or beginning stage of a proposed change, program, or assessment. Initial risk is determined by factoring both verified controls and assumptions into the system state. When assumptions are made, they must be documented as recommended controls. Once the initial risk is established, it is not changed.

3.13. Recommended Safety Requirements: The suggested mitigations or controls that have the potential to mitigate a hazard or risk but have not yet been validated or verified as part of the system or its requirements.

3.14. Organization Responsible for Implementing Safety Requirements: The organization's name and the point of contact's name and number.

3.15. Predicted Residual Risk: The term used until the safety analysis is complete and all safety requirements have been verified. Predicted residual risk is based on the assumption that all safety requirements will be validated and verified.

3.16. Safety Performance Targets: The measurable goals that will be used to verify the predicted residual risk of a hazard.

DATA ITEM DESCRIPTION

Title: Operating and Support Hazard Analysis
Number: AJI-DID-O&SHA-001 **Approval Date:** TBD
AMSC Number: N/A **Limitation:** N/A
DTIC Applicable: No **GIDEP Applicable:** No
Office of Primary Responsibility: Air Traffic Organization Safety and Technical Training, Integrated Safety Policy Team
Applicable Forms: N/A

Use/relationship:
The Operating and Support Hazard Analysis (O&SHA) is performed by the contractor primarily to identify and evaluate hazards associated with the interactions between humans and equipment/systems to ensure that procedures do not introduce new hazards. These interactions include all operations conducted throughout the lifecycle of the system. The purpose of the O&SHA is to perform a detailed systematic safety analysis that addresses hazards and risk applicable to the operation and support activities of a given system. It evaluates the effectiveness of controlling procedural hazards instead of only those hazards created by design. This encompasses operating the system (primarily procedural aspects) and the support functions (e.g., maintenance, servicing, overhaul, facilities, equipment, and training). The O&SHA may also be selectively applied to facilities acquisition projects to ensure that operation and maintenance manuals properly address safety and health requirements. The O&SHA is used to both identify new requirements and to support the verification and validation of existing requirements.

This Data Item Description (DID) contains the format, content, and preparation instructions for the O&SHA.

This DID supersedes FAA-DI-SAFT-105.

Requirements:

1. Reference Documents:
   - The Air Traffic Organization (ATO) Safety Management System (SMS) Manual
   - The Safety Risk Management Guidance for System Acquisitions (SRMGSA)

2. Format: The report must be prepared as a Safety Risk Management Document using the guidelines contained in the ATO SMS Manual.

3. Content: The O&SHA must be written in accordance with the requirements of the ATO SMS Manual and the SRMGSA. The description of each identified hazard must contain, at a minimum, the information prescribed in paragraphs 3.1 through 3.16.

   3.1. Hazard Name: Alpha-numeric identifiers will be used to track hazards through the verification and validation process. Unique identifiers must be created and marked for individual hazards, or sequences created for clustered hazards or subsets.

3.2. Hazard Description: A complete statement describing the hazard. The ATO SMS Manual defines a hazard as, “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.” A hazard is a condition that is a prerequisite to an accident or incident.

3.3. Cause(s): Events that result in a hazard or failure. Causes can occur by themselves or in combinations. They may include, but are not limited to, human error, latent failure, active failure, design flaw, component failure, and software error.

3.4. System State: An expression of the various conditions, characterized by quantities or qualities, in which a system can exist. System state is described for each individual hazard associated with the system (e.g., adverse weather and lighting conditions, such as day, dusk, and night). The system state will also include the activity under which the harm may occur (e.g., storage; shipping; installation; testing; maintenance; replacement; decommissioning; or phase of flight, such as en route or taxiing). Any given hazard may have a different risk level in each possible system state. Hazard assessment must consider all possibilities while allowing for all system states. In a hazard analysis, it is important to capture different system states when the end results lead to the application of different mitigations. System state must be defined in accordance with the ATO SMS Manual.

3.5. Existing Controls: The existing safeguards, safety features, protective devices, warnings, training, and procedures that control or eliminate risk. An existing safety control is a requirement that exists currently in the Federal Aviation Administration (e.g., controls that were previously defined in prior analyses) that is validated or verified to mitigate or manage the risk of a hazard’s effect or occurrence.

3.6. Existing Control Justification / Supporting Data: The explanation of how existing controls were validated and verified.

3.7. Effects: The real or credible harmful outcome(s) that can be expected if the hazard occurs in the defined system state.

3.8. Severity: The measure of how bad the results of an event are predicted to be. Severity is determined by the worst credible outcome. Less severe effects may be considered analytically in addition to this, but at a minimum, the most severe effects are to be considered. Do not consider likelihood when determining severity; determination of severity is independent of likelihood. Determine the severity classifications from the ATO SMS Manual.

3.9. Severity Rationale: The explanation of how the severity was determined.

3.10. Likelihood: Likelihood is an expression of how often an event is expected to occur. Severity must be considered in the determination of likelihood. Likelihood is determined by how often the resulting harm can be expected to occur at the worst credible severity. When determining likelihood, the worst credible system

states will usually determine the worst credible severity. Determine the likelihood classifications from the ATO SMS Manual.

3.11. Likelihood Rationale: The explanation of how likelihood was determined.

3.12. Initial Risk: The composite of the severity and likelihood of a hazard considering only verified controls and documented assumptions for a given system state. It describes the risk at the preliminary or beginning stage of a proposed change, program, or assessment. Initial risk is determined by factoring both verified controls and assumptions into the system state. When assumptions are made, they must be documented as recommended controls. Once the initial risk is established, it is not changed.

3.13. Recommended Safety Requirements: The suggested mitigations or controls that have the potential to mitigate a hazard or risk but have not yet been validated or verified as part of the system or its requirements.

3.14. Organization Responsible for Implementing Safety Requirements: The organization's name and the point of contact's name and number.

3.15. Predicted Residual Risk: The term used until the safety analysis is complete and all safety requirements have been verified. Predicted residual risk is based on the assumption that all safety requirements will be validated and verified.

3.16. Safety Performance Targets: The measurable goals that will be used to verify the predicted residual risk of a hazard.

DATA ITEM DESCRIPTION

Title: System Safety Assessment Report
Number: AJI-DID-SSAR-001 **Approval Date:** TBD
AMSC Number: N/A **Limitation:** N/A
DTIC Applicable: No **GIDEP Applicable:** No
Office of Primary Responsibility: Air Traffic Organization Safety and Technical Training, Integrated Safety Policy Team
Applicable Forms: N/A

Use/relationship:
The System Safety Assessment Report (SSAR) is a report to provide management with an overall assessment of the risk associated with the system prior to fielding and must be employed prior to operation of the system. This is accomplished by providing summaries of the analyses and testing results. The report contains an overall assessment of the program from the analyses performed and a status of all the existing and recommended safety requirements. The SSAR identifies all safety features of the system, the design and procedural hazards that may be present in the system being acquired, and the specific procedural controls and precautions that should be followed.

This Data Item Description (DID) contains the format, content, and preparation instructions for the SSAR.

This DID supersedes FAA-DI-SAFT-107.

Requirements:

1. Reference Documents:
   - The Air Traffic Organization (ATO) Safety Management System (SMS) Manual
   - The Safety Risk Management Guidance for System Acquisitions (SRMGSA)

2. Format: The report must be prepared as a Safety Risk Management Document using the guidelines contained in the ATO SMS Manual.

3. Content: The SSAR includes a summary of the analyses performed and their results, the tests conducted and their results, and the compliance assessment. The SSAR must contain the elements prescribed in paragraphs 3.1 through 3.8.

   3.1. Signature Page: Include the appropriate signature blocks for Risk Acceptance and Safety Risk Management Document Approval. This must be in accordance with the ATO SMS Manual.

   3.2. Executive Summary: A brief description of the scope of the assessment and the assessment findings, including the total number of high- and medium-risk hazards, controls, and other significant issues. The executive summary should also contain the total number of safety requirements (both existing and recommended), with requirements listed and discussed.

3.3. Safety Criteria and Methodology: A narrative summary of the total number of program hazards identified, as well as a breakdown of the high-, medium-, and low-risk hazards.

3.4. Risk Assessment Ratings: Results of the analyses plotted on the risk matrix.

3.5. Results of Analyses and Tests Performed (and Other Verification Activities): The summary and results of the analyses performed, as well as the tests conducted and the compliance assessment.

3.6. Hazards Identification: A list of all hazards along with specific recommended safety requirements. The list of hazards must be categorized according to whether or not they may be expected under normal or abnormal operating conditions.

The contractor system safety manager and the Service Team should sign a statement verifying that all identified hazards have been eliminated or controlled and that the system is ready to test, operate, or proceed to the next acquisition phase. In addition, include recommendations applicable to the safe interface of this system with other systems.

The Hazard Identification must demonstrate that system operations were performed by documenting:

- A description of or reference to the procedures for operating, testing, and maintaining the system. Discuss the safety design features and controls incorporated into the system as they relate to the operating procedures.
- A description of any special safety procedures needed to assure safe operations, testing, and maintenance, including emergency procedures.
- A description of the anticipated operating environments and any specific skills required for safe operation, testing, maintenance, transportation, or disposal.
- A description of any special facility requirements or personal equipment needed to support the system.

The Hazard Identification must demonstrate that systems safety engineering was performed by documenting:

- A description of or reference to the analyses and tests performed to identify hazardous conditions inherent in the system.
- A discussion of or reference to the results of tests conducted to validate safety criteria requirements and analyses.

3.7. List of Hazards (with Risk) Identified to Date: A list of all hazards by sub-system or major component level that have been identified and considered from the inception of the program. This should include a discussion of:

- The actions that have been taken to eliminate or control the individual hazards,

- The effects of the safety requirements on the likelihood and severity of the individual hazards, and
- The residual risks that remain after the recommended safety requirements are applied.

3.8. Safety Requirements Verification Table: Provide an updated list of safety requirements that have been verified, as well as a status of the requirements that still need to be verified and when they will be verified.

Appendix E

Acronyms and Abbreviations

AJI	ATO Safety and Technical Training
AJR	ATO System Operations Services
AJT	ATO Air Traffic Services
AJV	ATO Mission Support Services
AJW	ATO Technical Operations Services
AMS	Acquisition Management System
ANG	Office of NextGen
AOV	Air Traffic Safety Oversight Service
ARP	Office of Airports
ATM	Air Traffic Management
ATO	Air Traffic Organization
ATO-SG	Air Traffic Organization Safety Guidance
AVS	Office of Aviation Safety
CapSA	Capability Safety Assessment
CMTD	Concept Maturity and Technical Development
CNS	Communication, Navigation, and Surveillance
ConOps	Concept of Operations
CRD	Concept and Requirements Definition
CSA	Comparative Safety Assessment
CST	Capability Safety Team
DAL	Development Assurance Level
DID	Data Item Description
DTIC	Defense Technical Information Center
EA	Enterprise Architecture
EOSH	Environmental and Occupational Safety and Health
FA	Functional Analysis
FAA	Federal Aviation Administration
FAST	FAA Acquisition System Toolset
FID	Final Investment Decision
fPRD	Final Program Requirements Document
GIDEP	Government-Industry Data Exchange Program
GSIP	Generic Site Implementation Plan
IA	Investment Analysis
IAP	Investment Analysis Plan
IARD	Investment Analysis Readiness Decision
IID	Initial Investment Decision
IOA	Independent Operational Assessment
IOC	Initial Operating Capability
ISA	Independent Safety Assessment
ISD	In-Service Decision
ISM	In-Service Management
ISPD	Implementation Strategy and Planning Document
ISR	In-Service Review
ISRM	Integrated Safety Risk Management
ISSA	Integrated System Safety Assessment

JRC	Joint Resources Council
LOB	Line of Business
NAS	National Airspace System
NextGen	Next Generation Air Transportation System
NMB	NextGen Management Board
NSIP	NextGen Segment Implementation Plan
OI	Operational Improvement
ORM	Operational Risk Management
OS	Operational Sustainment
OSA	Operational Safety Assessment
O&SHA	Operating and Support Hazard Assessment
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PIR	Post-Implementation Review
PM	Program Manager
PMO	Program Management Organization
POC	Point of Contact
pPRD	Preliminary Program Requirements Document
PSAA	Plan for Software Aspects of Approval
PSP	Program Safety Plan
PST	Program Safety Team
SCT	Safety Collaboration Team
SEM	Systems Engineering Manual
SHA	System Hazard Analysis
SME	Subject Matter Expert
SMS	Safety Management System
SOC	Safety Oversight Circular
SRM	Safety Risk Management
SRMD	Safety Risk Management Document
SRMDM	Safety Risk Management Decision Memorandum
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
SSPP	Systems Safety Program Plan
SSW	Safety Strategy Worksheet
V&V	Verification and Validation