SRMGSA

Safety Risk Management Guidance for System Acquisitions

Air Traffic Organization March 2020

ALL POINTS/SAFETY
everyone. everywhere. everyday.

FAA
Air Traffic Organization

Contents

Preface

1. Introduction
- 1.1 Purpose
- 1.2 Scope
- 1.3 Changes to the SRMGSA

2. Safety Requirements in the Acquisition Management System Lifecycle
- 2.1 Acquisition Management
- 2.2 Integration of SRM and AMS
  - 2.2.1 System Safety Deliverables
  - 2.2.2 Approval Authority
- 2.3 Program Safety Requirements
  - 2.3.1 Achieving a CRDR Decision
  - 2.3.2 Achieving an IARD
    - 2.3.2.1 Safety Requirements
      - 2.3.2.1.1 EA Safety Roadmap
      - 2.3.2.1.2 PSP
      - 2.3.2.1.3 OSA
      - 2.3.2.1.4 System Development Assurance
      - 2.3.2.1.5 pPRD
      - 2.3.2.1.6 IAP
  - 2.3.3 Achieving an IID
    - 2.3.3.1 Safety Requirements
      - 2.3.3.1.1 PSP
      - 2.3.3.1.2 CSA
        - 2.3.3.1.2.1 System Development Assurance
      - 2.3.3.1.3 Initial Business Case
      - 2.3.3.1.4 Initial ISPD
      - 2.3.3.1.5 Preliminary TEMP
      - 2.3.3.1.6 PMP
  - 2.3.4 Achieving an FID
    - 2.3.4.1 Safety Requirements
      - 2.3.4.1.1 PSP
      - 2.3.4.1.2 PHA
        - 2.3.4.1.2.1 System Development Assurance
      - 2.3.4.1.3 fPRD
      - 2.3.4.1.4 Final Business Case
      - 2.3.4.1.5 Final ISPD
      - 2.3.4.1.6 Initial TEMP
      - 2.3.4.1.7 PMP
      - 2.3.4.1.8 PIR Strategy
  - 2.3.5 Achieving an ISD
    - 2.3.5.1 Safety Requirements
      - 2.3.5.1.1 PSP
      - 2.3.5.1.2 SSPP
      - 2.3.5.1.3 System Development Assurance
        - 2.3.5.1.3.1 Development Assurance Documents (System, Hardware, Software)

2.3.5.1.3.2 Development Assurance: Evidence of Compliance
2.3.5.1.3.3 Development Assurance: Audit Results
2.3.5.1.4 SSHA
2.3.5.1.5 SHA
2.3.5.1.6 O&SHA
2.3.5.1.7 Final TEMP
2.3.5.1.8 GSIP
2.3.5.1.9 NAS Change Proposal
2.3.5.1.10 PIR Plan
2.3.5.1.11 SSAR
2.3.6 ISM
2.3.6.1 Post-Implementation Safety Assessment
2.3.6.2 PIR Report
2.4 TR Portfolio Safety Requirements

3. References

4. Roles and Responsibilities
4.1 JRC Executive Secretariat
4.1.1 Portfolio Stakeholders Governing Body
4.2 Assistant Administrator for ANG and NextGen Portfolio Management
4.3 Office of Aviation Safety
4.4 Safety Collaboration Team
4.5 ATO
4.5.1 SU Roles and Responsibilities
4.5.2 PO Roles and Responsibilities
4.5.2.1 PST
4.5.3 AJM Roles and Responsibilities
4.5.4 ATO Chief Safety Engineer Roles and Responsibilities
4.5.5 AJI Roles and Responsibilities
4.5.5.1 AJI Safety Engineering Team Manager
4.5.5.2 AJI SCLs
4.5.5.3 AJI Audits and Assessments Group
4.5.5.4 ISD Executive Secretariat

5. Safety Planning for Acquisitions
5.1 Portfolio Safety Strategy
5.2 Safety Strategy Meetings and Program Safety Plans
5.2.1 Consistency with the Implementation Strategy and Planning Document
5.2.2 Technology Refreshment Portfolio

6. Other Considerations
6.1 Baseline Change Management
6.2 Program Safety Requirements for Decommissioning and Disposal
6.3 Managing Software Risk
6.4 Site Implementation
6.5 Legacy System SRM
6.6 Physical Security, Information Security, Cybersecurity, and Occupational Safety and Health
6.6.1 Safety and Security Issue Reporting
6.7 COTS Products
6.8 Safety Performance Targets and Monitoring Plans

6.9 Program Segmentation
6.10 Program Risk Management

7. Equivalent Processes

8. Safety Risk Management Documentation, Approval, and Tracking
8.1 Safety Risk Management Documents
8.2 Mission Support Programs
8.3 Peer Review Process
8.4 Approval Authorities and Coordination Requirements
8.5 SMTS

9. System Safety Considerations
9.1 System Safety
9.2 Integrated Safety Management
9.3 FAA / System Developer Interface
9.4 Software-Intensive Systems
9.4.1 System Development Assurance
9.4.1.1 Determining the Development Assurance Level
9.4.1.2 RTCA DO-278A Compliance Gap Analysis
9.4.1.3 Software Approval Process

Appendices

Appendix A: Guidance for Preparing and Implementing Program Safety Plans

Appendix B: Description and Overview of the System Safety Program Plan

Appendix C: Guidance for Conducting and Documenting an Operational Safety Assessment

Appendix D: Guidance for Conducting and Documenting a Comparative Safety Assessment

Appendix E: Guidance for Conducting and Documenting a Preliminary Hazard Analysis

Appendix F: Guidance for Conducting and Documenting a Sub-System Hazard Analysis

Appendix G: Guidance for Conducting and Documenting a System Hazard Analysis

Appendix H: Guidance for Conducting and Documenting an Operating and Support Hazard Analysis

Appendix I: Guidance for Documenting a System Safety Assessment Report

Appendix J: Development Assurance for Communication, Navigation, Surveillance and Air Traffic Management Systems

Appendix K: Conducting an RTCA DO-278A Software Assurance Compliance Analysis for Acquired National Airspace System Systems

Appendix L: Software Assurance Approval Guidelines for Communication, Navigation, Surveillance and Air Traffic Management Systems

Appendix M: Overview of RTCA DO-278A and Its Required Deliverables

Appendix N: Acronyms

Preface

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

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

1 Introduction

The Safety Risk Management Guidance for System Acquisitions (SRMGSA) defines the scope, purpose, objectives, and required activities of the Federal Aviation Administration (FAA) system safety effort as it applies to Safety Risk Management (SRM) for all system acquisitions that provide Communication, Navigation, and Surveillance; Air Traffic Management; and other services in the National Airspace System (NAS).[1] The SRMGSA applies to all personnel in the Air Traffic Organization (ATO) performing SRM analyses/assessments on system acquisitions and is of interest to the Assistant Administrator of the Office of NextGen (ANG), the Office of Airports, and 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 labor, and
- The fostering of personal accountability and corporate self-regulation in safety matters.

1.1 Purpose

The SRMGSA provides a framework and further process definition to execute SRM throughout the entire lifecycle of a system or product. This framework is made formal in the Program Safety Plan (PSP) developed by the Program Office (PO) and the system developer's System Safety Program Plan (SSPP), as contractually required. (Refer to Appendix A for guidance on developing and implementing PSPs. Refer to Appendix B for a description of the SSPP that the system developer submits.) The SRMGSA follows systems engineering principles to achieve the SRM objectives defined in the various FAA publications listed in Section 3.

The purpose of the SRMGSA is to meet the requirements of and implement the policy stated in FAA Acquisition Management System (AMS), Section 4.12, *National Airspace System Safety Management System*. This section of the AMS requires the application of a Safety Management System (SMS), referring to the ATO SMS Manual and the SRMGSA as governing documents with which compliance is mandatory. Therefore, the SRMGSA provides the guidelines that must be used by the ATO and other organizations when conducting SRM in acquisitions. In addition, FAA Order 1100.161, *Air Traffic Safety Oversight*, focuses the Air Traffic Safety Oversight Service's (AOV's) efforts on the acquisition and implementation of new systems to include the modernization/upgrade of legacy NAS systems. Per AOV Safety Oversight Circular 09-11, *Safety Oversight Standards*, new acquisitions are required to follow the guidance of the AMS and meet the program requirements defined in the SMS Manual and the SRMGSA.

The conduct of SRM maintains or improves the safety of the NAS by identifying the safety risk associated with making NAS changes and providing that input to decision makers responsible for managing and mitigating this safety risk. When system[2] safety hazards are identified, 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 the NAS Enterprise Architecture Portal.

2. The current version of FAA Order 8040.4, *Safety Risk Management Policy*, defines a system as an integrated set of constituent elements that are combined in an operational or support environment to accomplish a defined

subsequent mitigations derived from the SRM process (as described in the SMS Manual) are translated into requirements for the acquired systems.

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

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

The SRMGSA provides the following:

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

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

When a change to AMS policy, the SMS Manual, or FAA/ATO management direction affects the accepted scope of performance or requirements of the SRMGSA, the SRMGSA may be revised

objective. These elements include people, hardware, software, firmware, information, facilities, services, and other support facets.

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

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

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

upon agreement among AJI, the Program Management Organization, the ATO Chief Safety Engineer, and the Acquisition Systems Advisory Group.

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.[6] AMS policy, FAA orders, and the SMS Manual mandate a planned and organized SRM approach to RBDM that is consistent with the role of each organization in the FAA.

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

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

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

1.3 Changes to the SRMGSA

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

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

2 Safety Requirements in the Acquisition Management System Lifecycle

2.1 Acquisition Management

Federal Aviation Administration (FAA) Acquisition Management System (AMS), Section 4.12, *National Airspace System Safety Management System*, contains the AMS policies for the safety management of National Airspace System (NAS) acquisitions. This section requires that:

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

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

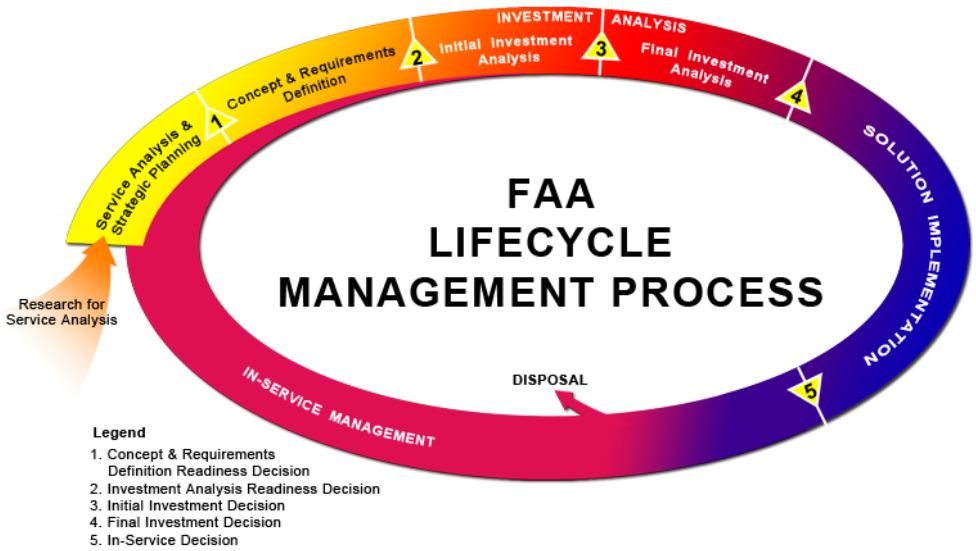

Figure 2.1: FAA Lifecycle Management Process

2.2 Integration of SRM and AMS

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

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

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

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

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

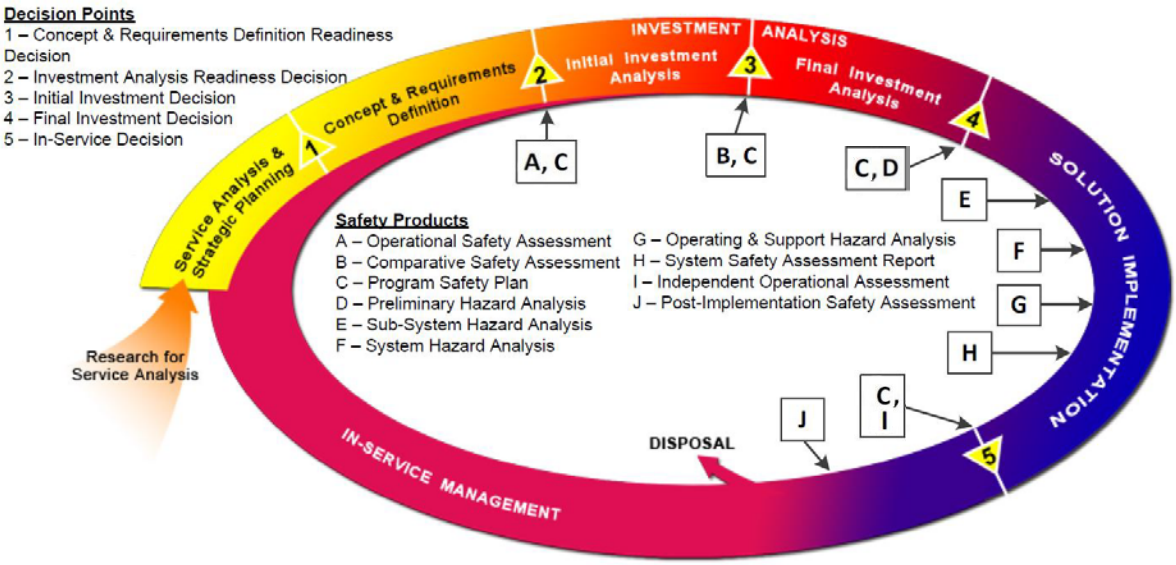

Figure 2.2: FAA Lifecycle Management Process (with Safety Deliverables)

2.2.1 System Safety Deliverables

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

2.2.2 Approval Authority

No one FAA organization has total approval authority. The PO is responsible for product approval (i.e., deciding whether the developer has complied with the contract). The JRC has funding approval (i.e., deciding whether to fund a project). The safety risk acceptor has performance approval (i.e., deciding if the system's performance is adequate (regardless of whether the developer has complied with the contract)). Safety and Technical Training (AJI) maintains the safety approval role (i.e., ensuring all system safety requirements are met). Each approver has the authority to prevent the deployment of a system. This separation of approval authority guarantees that checks and balances exist among lines of business that each have

different goals. Approval is a shared responsibility, and each approving entity has the right to request the necessary documentation to perform its role.

The Program Management Organization (AJM) (not the ATO Chief Safety Engineer) is responsible for approving the following safety deliverables: the System Hazard Analysis (SHA), the Sub-System Hazard Analysis (SSHA), and the Operations and Support Hazard Analysis (O&SHA). Similarly, AJM is responsible for approving the following deliverables related to RTCA[1] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*: the Plan for Software Aspects of Approval, Software Configuration Indexes, and the Software Accomplishments Summary.

Table 2.1 identifies the organization(s) responsible for producing and approving each deliverable.

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

Table 2.1: ATO System Safety Deliverables

Acquisition Phase	Deliverables*	Reference	Responsibility	Required Approval	AMS Decision Point
Service Analysis and Strategic Planning	This phase is not covered by the Safety Risk Management Guidance for System Acquisitions (SRMGSA)				Concepts and Requirements Definition Readiness (CRDR) Decision
Concepts and Requirements Definition (CRD)	Enterprise Architecture (EA) Safety Roadmap	AMS	Office of NextGen (ANG) / Mission Support Services (AJV) / PO	ANG	Investment Analysis Readiness Decision (IARD)
	Program Safety Plan (PSP)	SRMGSA Appendix A	ANG//PO	AJI	
	SRM Document: Operational Safety Assessment (OSA)	SRMGSA Appendix C	ANG/AJV/PO	AJI	
	System Development Assurance	AMS	ANG/PO	AJI	
	Preliminary Program Requirements Document (pPRD)	AMS	ANG/PO	PO	
	Execution Plan (for TR portfolios)	AMS	PO	PO	
	Investment Analysis Plan (IAP)	AMS	PO	PO	
Initial Investment Analysis (IA)	Updated PSP (if needed)	SRMGSA Appendix A	PO	AJI	Initial Investment Decision (IID)
	SRM Document: Comparative Safety Assessment (CSA)	SRMGSA Appendix D	PO	AJI	
	Initial Business Case	AMS	PO	PO	
	Initial Implementation Strategy and Planning Document (ISPD)	AMS	PO	PO/AJI**	
	Preliminary Test and Evaluation Master Plan (TEMP)	AMS	PO	PO	
	Program Management Plan (PMP)	AMS	PO	PO	
Final IA	Updated PSP (if needed)	SRMGSA Appendix A	PO	AJI	Final Investment Decision (FID)
	SRM Document: Preliminary Hazard Analysis (PHA)	SRMGSA Appendix E	PO	AJI	
	Final Program Requirements Document (fPRD)	AMS	PO	PO	
	Final Business Case	AMS	PO	PO	
	Final ISPD	AMS	PO	PO/AJI**	
	Initial TEMP	AMS	PO	PO	
	Updated PMP	AMS	PO	PO	
	Post-Implementation Review (PIR) Strategy	AMS	PIR Team	PIR Team	
Solution Implementation (SI)	System Safety Program Plan (SSPP)	SRMGSA Appendix B	Developer	PO	Initial Operating Capability (IOC) / ISD
	Development Assurance Evidence of Compliance: Planning Review	SRMGSA Appendix J and L	PO	AJI	
	SRM Document: SSHA	SRMGSA Appendix F	PO/Developer	PO	
	SRM Document: SHA	SRMGSA Appendix G	PO/Developer	PO	
	SRM Document: O&SHA	SRMGSA Appendix H	PO/Developer	PO	
	Final TEMP	AMS	PO	PO	
	Development Assurance: Evidence of Compliance (Results of Reviews)	SRMGSA Section 4.5.5.3 and Appendix L	PO	AJI	

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

*Safety deliverables may be tailored in a PSP.

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

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

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

2.3 Program Safety Requirements

2.3.1 Achieving a CRDR Decision

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

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

The Safety Collaboration Team (SCT) was appointed by the FAA SMS Committee to facilitate the integrated safety management of pre-decisional NAS changes affecting the FAA. In doing so, the committee recognized the need to ensure that safety is not compromised when the FAA proposes pre-decisional changes that affect NAS operations. SCT activities are outside the scope of the SRMGSA.

2.3.2 Achieving an IARD

The IARD occurs at the end of the CRD phase. At the IARD, the JRC determines whether the ConOps, preliminary requirements, EA products and amendments, and preliminary program investment 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. CRD phase activities occur prior to the establishment of clear functions, baseline requirements, alternative solutions, and solution design.

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

2.3.2.1 Safety Requirements

2.3.2.1.1 EA Safety Roadmap

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

2.3.2.1.2 PSP

The PSP is the PO’s plan for the program’s safety process. The PSP is used to ensure compliance with provisions of the ATO SMS Manual and the SRMGSA. The PO must adjust

the PSP to the specific needs and SRM requirements of the program consistent with the phase of the AMS lifecycle that the program is entering. The tailoring of the PSP must be in accordance with agreements made at the Safety Strategy Meeting (SSM) (refer to Section 5.2 for details). 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 requesting an IARD. The PSP supports the IARD and is completed and approved prior to the JRC Secretariat's cut-off date for the IARD. Early in the acquisition lifecycle, the PSP may be very high level as many of the program specifics are not yet known. The PO further develops the PSP as the acquisition process matures.

The PSP must include the PO's methodology and approach to meeting the development assurance safety requirements.

See Appendix A for further details on preparing a PSP.

2.3.2.1.3 OSA

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

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

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

See Appendix C for further details on preparing an OSA.

2.3.2.1.4 System Development Assurance

Section 2.2.1.2 of the SMS Manual requires designers of NAS hardware and software to design systems that will not impose hazardous conditions during abnormal performance. AMS, Section 4.12, requires programs (e.g., systems, hardware components, and software components) to conduct product development at a rigor commensurate with the severity of the resultant hazard should that product experience failure. This may result in different

Development Assurance Levels (DALs) for different hardware and software components. See Appendix J for further information about DALs.

Development assurance is a safety requirement that must be approved by AJI. The aviation industry standards that address system development assurance are:

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

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

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

AMS, Section 4.12, specifically identifies the guidance/standards in RTCA DO-278A as the recommended means to accomplish software design rigor. If not using RTCA DO-278A, the PO must propose an equivalent approach that meets the AMS requirement(s) for software design rigor.

Compliance with SAE ARP4754A and RTCA DO-254 is not specifically required; other similar standards may be equally valid. Regardless, the PO must propose an approach that meets the AMS requirement for system, hardware, and software rigor.

2.3.2.1.5 pPRD

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

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

2. An ARP is a guideline from SAE International.

2.3.2.1.6 IAP

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

2.3.3 Achieving an IID

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

2.3.3.1 Safety Requirements

2.3.3.1.1 PSP

Prior to receiving an IID decision, the PO must update the PSP (if needed) with the latest information. At this phase of the acquisition lifecycle, there could be changes to the management and safety team as the program moves from ANG to ATO control.

2.3.3.1.2 CSA

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

The expanded PHL is developed from the FA or FHA, at which point each hazard's risk is assessed in the context of the alternatives. After this is done, requirements and recommendations can be made based on the data in the CSA. The PO must write the CSA in a manner in which the decision maker can clearly distinguish the safety merit of each alternative.

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

See Appendix D for further information on preparing a CSA.

2.3.3.1.2.1 System Development Assurance

The DAL is validated in the CSA, which may differ among investment alternatives. The DALs for the alternatives are then included in the IAP and ISPD prior to the IID.

2.3.3.1.3 Initial Business Case

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

2.3.3.1.4 Initial ISPD

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

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

2.3.3.1.5 Preliminary TEMP

The TEMP is the primary test management document for an acquisition program throughout its lifecycle. It delineates all activities that must be performed to achieve the goals of Verification and Validation (V&V). It also documents the Test and Evaluation (T&E) methodologies that will be used to assess safety hazard controls and security risks. The preliminary TEMP describes the investment program test strategy and scope. It is developed based upon the concepts and functions documented in the pPRD prior to the IID and is not expected to contain the complete level of detail required to fully implement the T&E program.

2.3.3.1.6 PMP

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

2.3.4 Achieving an FID

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

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

This early assessment allows for informed, data-driven decisions.

To support the FID, a PHA is completed to inform the PO and JRC of the risk ratings for the program. The required work products of the Final IA phase must be verified and validated (according to the AMS V&V guidance) prior to the FID. If the JRC accepts the recommendations, it approves the investment program for implementation; delegates

responsibility to the appropriate service organization; and approves the fPRD, final Business Case, and the final ISPD, all of which take safety into account.

2.3.4.1 Safety Requirements

2.3.4.1.1 PSP

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

2.3.4.1.2 PHA

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

The PO conducts the PHA with input from the OSA, CSA, FHA, FA, and/or models such as the Bow-Tie Model. It is important to note that the OSA and CSA may not have been performed if the ATO Chief Safety Engineer waived the requirement to perform those assessments. Although an FA, FHA, and/or Bow-Tie Model is not required, they are all highly recommended as tools that can assist in the hazard identification process and subsequent portions of the analysis. A human reliability analysis or assessment may also be conducted.

The PO conducts the PHA after the JRC has selected a single alternative as the best option. This means it is conducted after the CSA is approved and before the FID. The SRM document must be completed and approved prior to the JRC Secretariat's cut-off date for the FID. The PHA also becomes the basis of the monitoring plan that must be followed after system deployment.

See Appendix E for further information on preparing a PHA.

2.3.4.1.2.1 System Development Assurance

The final DALs are determined from the PHA and included in the fPRD and PSP. The impact of any changes to the DALs must be described in the final versions of the Business Case and ISPD prior to the FID.

2.3.4.1.3 fPRD

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

Changes in the NAS environment in which the new capability is targeted to operate may evolve while solution development takes place. Setting baselines of requirements, design, production, and "as-built" configuration makes fulfilment of new safety needs more expensive under this original program segment or capability increment. Future investment segments, increments,

options, and contingencies may be recognized to reorganize solution development into phases. Actual residual risk may be higher or lower depending on the sum total of all outside influences and developments in NAS operations during the years it takes to field the new system.

2.3.4.1.4 Final Business Case

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

2.3.4.1.5 Final ISPD

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

2.3.4.1.6 Initial TEMP

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

2.3.4.1.7 PMP

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

2.3.4.1.8 PIR Strategy

A PIR is an evaluation tool used to assess the results of an investment program against baseline expectations 6 to 24 months after the program goes into operational service. The PIR's main objective is to assess an investment program, determining whether the program is achieving expected performance and benefit targets, meeting the service needs of customers, and upholding the validity of the original Business Case. The PIR process is governed by AMS Section 4.15.1, *Post-Implementation Review*.

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

2.3.5 Achieving an ISD

At the end of the SI phase, the PO must obtain an ISD that authorizes deployment of a solution into the operational environment and occurs after demonstration of the IOC[3] at the key site.

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

The ISD establishes the foundation for the declaration of operational readiness at the key site and IOC at subsequent sites. The PO must submit an approved SRM document (typically, an SSAR, unless otherwise directed by the ATO Chief Safety Engineer) at the IOC; it must be updated prior to the ISD to reflect national deployment. Additionally, prior to the ISD, all of the safety-related ISR checklist items must be closed or have an approved Action Plan.

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

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

The PO must complete the full suite of safety analyses required by the ATO, and all of these analyses must be listed in the approved PSP. Typical safety analyses, usually performed by the prime vendor or its subcontractor, are listed in Table 2.1.

2.3.5.1 Safety Requirements

2.3.5.1.1 PSP

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

2.3.5.1.2 SSPP

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

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

2.3.5.1.3 System Development Assurance

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.

2.3.5.1.3.1 Development Assurance Documents (System, Hardware, Software)

Throughout the SI phase, the developer will generate many development assurance documents as required by the standards followed. For example, RTCA DO-278A identifies 22 documents that must be generated during software development.

2.3.5.1.3.2 Development Assurance: Evidence of Compliance

The PO must review and approve all developmental assurance documents and compare them to the standards followed to verify whether the developer complied with the appropriate level of

rigor as dictated by the DAL. As a result, the PO will generate reports or checklists documenting the evidence of compliance, which will be submitted to AJI.

AJI may request copies of documents in order to evaluate the submitted evidence. AJI will review and approve the PO's evidence, determining whether it sufficiently proves that the system complies with the PSP. For software, evidence of the following reviews must be submitted:

- Software planning review,
- Software development review,
- Software verification review, and
- Final software review.

See Appendix L for further information on the above-listed reviews.

2.3.5.1.3.3 Development Assurance: Audit Results

Appendix L describes the level of approval authority involvement. Based on the evidence of compliance provided by the PO, the Audits and Assessments Group, AJI-32, will audit the development to provide an independent evaluation of compliance with the PSP. An audit will be performed for any new project. For projects that are modifications to existing systems, the team will analyze the scope of the change and determine if the results of the previous audit are sufficient. If a new audit is deemed unnecessary, then AJI will prepare an analysis report.

2.3.5.1.4 SSHA

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

See Appendix F for further information on preparing an SSHA.

2.3.5.1.5 SHA

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

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

The SHA should begin as the system design matures at the preliminary design review or at the facilities concept design review milestone. It should be updated until the design is complete. If new safety hazards are identified in the SHA (i.e., safety hazards that are not previously

described in or cannot be traced back to the PHA), then the PHA must be updated to include them.

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

2.3.5.1.6 O&SHA

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

The O&SHA identifies hazards and risks occurring during operation of the system. This primarily encompasses the procedural aspects as well as the support functions (e.g., maintenance, servicing, overhaul, facilities, equipment, and training). Its purpose is to evaluate the effectiveness of mitigating procedural hazards (not hazards created by design). Additionally, the O&SHA 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 T&E. As a result, the O&SHA is typically the last formal analysis to be completed, usually mid-way through the SI phase. The sooner the analysis can begin, the better. Even before the system is designed, an O&SHA can begin identifying hazards within the anticipated operation of the system. Ideally, the O&SHA should begin with the formulation of the system and not be completed until sometime after its initial test (which may identify additional hazards). 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 POs and users to accept unnecessary risk. If new safety hazards are identified in the O&SHA (i.e., safety hazards that are not previously described in or cannot be traced back to the PHA), then the PHA must be updated to include them.

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

2.3.5.1.7 Final TEMP

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

2.3.5.1.8 GSIP

POs must develop GSIPs in accordance with the current version of FAA Order JO 6000.50, *National Airspace System (NAS) Integrated Risk Management,* for all construction and/or installation activities they sponsor. POs must develop an SRM document for any GSIP.

2.3.5.1.9 NAS Change Proposal

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

2.3.5.1.10 PIR Plan

The PIR Team must develop a PIR Plan prior to the ISD for the investment program under review. The plan must expand and refine the PIR Strategy by defining expected outcomes, planned activities, and resources necessary to complete the review. SRM input to the plan should be submitted after the SSAR is completed and approved. The 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.

2.3.5.1.11 SSAR

The purpose of an SSAR is to conduct and document a comprehensive evaluation of the safety risk being accepted before the program is deployed into the NAS. This means that the SSAR summarizes the safety analyses and assessments and development assurance activities conducted by the PO. 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, SSHA, SHA, and O&SHA), including V&V. At the IOC and ISD, all safety requirements must undergo V&V by the PO. Objective evidence of V&V closed status may be reviewed by the ATO Chief Safety Engineer upon request.

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

While verifying the safety requirements, AJI may review all of the previous development assurance activities to make a final determination that the development assurance safety requirements have been met.

When the ATO Chief Safety Engineer approves the SSAR, he or she affirms that all safety requirements have been met.

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

2.3.6 ISM

2.3.6.1 Post-Implementation Safety Assessment

After a system's IOC and/or ISD, the Operational Audits and Assessments (Air Traffic) Team, AJI-323, may perform a post-implementation safety assessment. AJI-323 must transmit any safety-related findings to the PO for action.

2.3.6.2 PIR Report

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

After the PIR Report is completed, the PO must develop a plan outlining actions and milestones (with completion dates) to address the report's recommendations. These recommendations

support the ISM phase of the AMS lifecycle and are reported to the investment decision authority; impacted Vice Presidents or equivalent; and key stakeholders, including AJI.

2.4 TR Portfolio Safety Requirements

A TR portfolio consists of two or more TR projects. Each TR project will be assigned to a sub–Acquisition Category (ACAT) of either "1" or "2" based on project cost.[4] Prior to the IARD, the TR Portfolio Manager must develop a portfolio PSP in accordance with Appendix A, which must be approved by the ATO Chief Safety Engineer. To facilitate this effort, the TR Portfolio Manager must contact the AJI SCL and conduct an SSM prior to developing the portfolio PSP to assist in tailoring any safety documentation requirements. It is possible that the complexity of some sub-ACAT 1 TR projects warrants the development of project-specific PSPs to supplement the portfolio PSP; this need must be detailed in the approved portfolio PSP. There is no need to develop project-specific PSPs for sub-ACAT 2 TR projects as the portfolio PSP would outline the SRM and development assurance requirements for these projects.

After the IARD, each sub-ACAT 1 TR project must follow the lifecycle process presented in Figure 2.2 per the Execution Plan (EP)[5] approved by the JRC at the IARD. However, the safety documentation required and development assurance requirements (as listed in Table 2.1) may be tailored; this will be decided during the SSM and reflected in the approved portfolio PSP (or in an approved project-specific PSP if necessary). (For example, will any sub-ACAT 1 projects require that an OSA be conducted?) The portfolio PSP (or an approved project-specific PSP, if necessary) must specify what decision points will be held (most likely an ISD) before the product can be deployed to service delivery points. If this tailoring is not documented in the approved portfolio PSP (or in an approved project-specific PSP if necessary), then the approved portfolio PSP must be revised. Before a product can be deployed, the ATO Chief Safety Engineer must approve an SSAR.

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

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

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

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

3 References

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

- The ATO Safety Management System Manual;
- The FAA Acquisition Management System / FAA Acquisition System Toolset;
- FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*;
- FAA Order 8040.4, *Safety Risk Management Policy*;
- FAA Order 1100.161, *Air Traffic Safety Oversight*;
- FAA Order 6032.1, *National Airspace System (NAS) Modification Program*;
- FAA Order JO 1030.1, *Air Traffic Organization Safety Guidance*;
- FAA Order JO 6000.50, *National Airspace System (NAS) Integrated Risk Management*;
- FAA Order 1370.121, *FAA Information Security and Privacy Program & Policy*;
- FAA Systems Engineering Manual;
- Air Traffic Safety Oversight Service (AOV) Safety Oversight Circular (SOC) 09-11, *Safety Oversight Standards*;
- AOV SOC 07-02, *AOV Concurrence/Approval at Various Phases of Safety Risk Management Documentation and Mitigations for Initial High-Risk Hazards*;
- AOV SOC 07-05A, *Guidance on Safety Risk Modeling and Simulation of Hazards and Mitigations*;
- ATO Safety Guidance (ATO-SG) ATO-SG-17-01, *Configuration Management for the Air Traffic Organization Safety Management System Policy*;
- RTCA[1] DO-178C, *Software Considerations in Airborne System Equipment Certification*;
- RTCA DO-248C, *Supporting Information for DO-178C and DO-278A*;
- RTCA DO-254,
- RTCA DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*;
- RTCA DO-330, *Software Tool Qualification Considerations*;
- RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A*;
- RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*;
- RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*; and

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

- SAE Aerospace Recommended Practice (ARP)[2] ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*.

2. An ARP is a guideline from SAE International.

4 Roles and Responsibilities

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

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

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.

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

4.1 JRC Executive Secretariat

The JRC Executive Secretariat maintains the AMS-based JRC Readiness Criteria Checklist, which ensures that the appropriate SRM documents required for all investment decisions have been coordinated with Safety and Technical Training (AJI). The ATO Chief Safety Engineer determines the completion of SRM documentation for programs progressing through the AMS

and advises the JRC Secretariat as to his or her decision.[1] The JRC has funding approval for the FAA and can decide whether to fund a project.

4.1.1 Portfolio Stakeholders Governing Body

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

4.2 Assistant Administrator for ANG and NextGen Portfolio Management

Next Generation Air Transportation System (NextGen) portfolios are typically organized into Operational Improvements (OIs), current operations,[2] increments, and procedure and documentation changes, which must all be combined to deliver the required services and capabilities. To provide a complete picture of the potential safety risk of fielding a particular capability (e.g., an OI), Integrated Safety Management must be conducted across that capability. The NextGen Investment Portfolio Leads are responsible for all aspects of their portfolio, including the conduct of Integrated Safety Management.

Some portfolios may have more than one FAA organization responsible for implementing their capabilities. The Office of NextGen (ANG) obtains work scope agreements from the operational Service Units (SUs) (e.g., Air Traffic Services (AJT) and System Operations Services (AJR)) through the Program Management Organization (AJM). Mission Support Services (AJV) supports NextGen portfolios (especially the validation of complete sets of requirements) during the Concept and Requirements Definition (CRD) phase and brings together AJR/AJT inputs. The Program Office (PO) provides transitional support during the Investment Analysis phase and full control of the Solution Implementation phase, and Technical Operations (AJW) provides support during the In-Service Management (ISM) phase.

The PO, AJV, and AJW must conduct SRM work at the solution, procedure, and document change levels by following the SRM process described in the SMS Manual. However, at the capability level, the ANG NextGen Investment Portfolio Leads are responsible for ensuring the conduct of safety assessments. The Portfolio Leads typically seek the assistance of the Enterprise Safety and Information Security Division, ANG-B3; the PO; and AJI in conducting these assessments. In the conduct of Integrated Safety Management, it is particularly important to properly set the scope of the safety assessments as there are numerous complex relationships among systems, procedures, OIs, and current operations. 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. As such, the NAS Enterprise Architecture (EA) should set the scope, which also supports tracing analysis results to NAS EA elements. Such traceability to NAS systems, functions, operational activities, etc. facilitates follow-on Integrated Safety Management efforts.[3]

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

2. A “current operation” is a fielded activity needed to sustain NAS services.

3. The purpose of the NAS EA is to establish the foundation from which evolution of the NAS can be explicitly understood and modeled.

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 IARD) 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; and
- Gather data on, understand, and articulate the safety issues/concerns as a capability evolves and moves through the acquisition lifecycle.

ANG has developed three SRM tools:

- An **Integrated System Safety Assessment (ISSA)** assesses changes in safety risk resulting from the implementation of NextGen OIs. The ISSA Report serves as a foundational safety document that will feed into other safety analysis activities through the course of the program lifecycle process.
- A **Service-Level Safety Assessment** is a means to assess current safety risk and provide a baseline for subsequent changes to the NAS.
- The **Hazard Enterprise Architecture Traceability (HEAT)** tool provides an interactive platform that allows users to search for available safety data via the FAA EA element connected to the subject of their safety analyses/assessments. The HEAT tool is located in the NAS Systems Engineering Portal.

4.3 Office of Aviation Safety

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

4.4 Safety Collaboration Team[5]

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

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

5. Excerpted from the Safety Collaboration Team Charter signed June 5, 2018.

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

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

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

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

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

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

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

The processes and procedures used by these workgroups and the SCT are beyond the scope of the Safety Risk Management Guidance for System Acquisitions (SRMGSA).

4.5 ATO

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

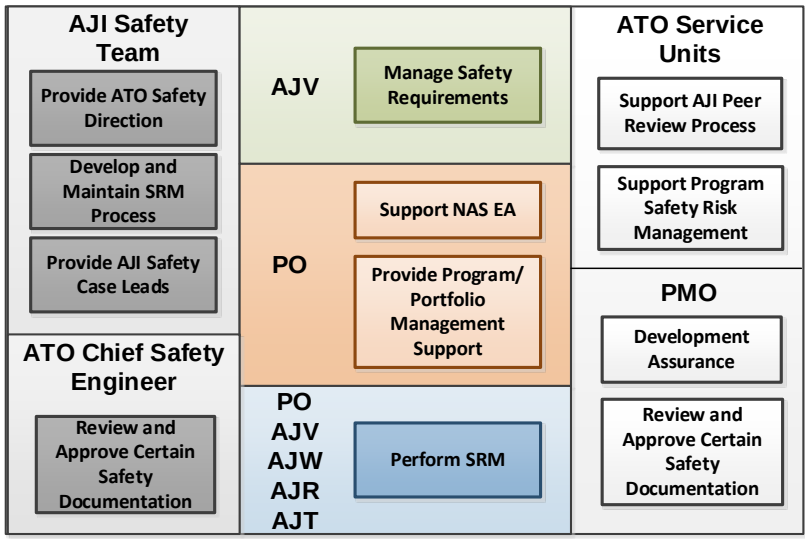

Figure 4.1: ATO Roles and Responsibilities

4.5.1 SU Roles and Responsibilities

Depending on the acquisition phase of the program, the PO, AJV, or AJW has the responsibility to ensure that SRM has been conducted and the necessary documentation has been prepared. They are supported as appropriate by subject matter experts from the PO, AJM, AJR, AJT, and/or AJW. Safety professionals within AJI also support the PO in preparing the safety documents and representing their functional discipline at reviews with the ATO Chief Safety Engineer. The SU representatives to the PO ensure that the SU Vice Presidents are informed of the risks involved with a proposed change to the NAS and recommend that they approve SRM documentation and accept risk in accordance with the SMS Manual, as necessary.

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

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

The NAS EA contains roadmaps that describe the transition from the "as-is" to the "to-be" environment. Roadmaps align the FAA's mission, benefits, and capabilities with its investments. Within the ATO, the PO 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 planning for the application of the SMS in all ATO-managed acquisition programs. The EA also contains architectural "as-is" and "to-be" views that govern the expected architecture, threaded features, levels, functional flow,

dependencies, and holistic performance of the NAS to be allocated among integral groups of dependent NAS systems. EA views, more so than roadmaps, help control the impacts of change among NAS systems.

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

4.5.2 PO Roles and Responsibilities[7]

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

When forming a Program Safety Team (PST), the PO 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 and monitoring results.

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

For SRM efforts conducted as part of the AMS process, the PO should hold a meeting with the ANG Enterprise Safety Team (EST)[8] to review any relevant enterprise safety assessments and HEAT reports and to assist with SRM compliance.

7. For information regarding the roles and responsibilities of POs not part of the ATO, contact the Safety Engineering Team, AJI-314.

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

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

4.5.2.1 PST

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

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

The PST must:

- Provide a central Point of Contact (POC) to coordinate all safety analyses throughout the program's lifecycle;
- Participate in Safety Strategy Meetings (SSMs) to determine the safety effort required in support of the AMS milestone decisions;
- Support the safety analyses in accordance with the guidelines in the AMS FAST, the SMS Manual, ATO Safety Guidance (ATO-SG) documents, and the SRMGSA;
- Submit the proposed Program Safety Plan (PSP) and completed SRM documents to the AJI SCL for review and coordination to ensure timely decisions in support of JRC milestone decisions;
- Ensure the developer's contract includes provisions to support AMS development assurance safety requirements;
- Review all development assurance documents to include RTCA[10] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*, (or equivalent document) lifecycle data;
- Enter required safety documentation into the Safety Management Tracking System (see Section 8.5 for more information);
- Address any safety analysis and assessment results in program planning and requirements documents;
- Incorporate any safety issues identified by the SCT or ANG EST into program safety efforts;
- Include any requirements developed as a result of the safety analyses as discrete requirements in the preliminary Program Requirements Document (PRD), the initial PRD, or the final PRD;
- Trace the safety requirements back to identified safety hazards;
- Verify that the mitigations identified to reduce safety risk are included as validated and verified safety requirements in the final SRM document;
- Support the establishment of traceability between safety analysis results and the NAS EA;
- Maintain safety documentation throughout the system lifecycle;

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

- Include SRM results in investment decision briefings to the JRC; and
- Coordinate the peer review process with the AJI SCLs. (See Section 8.3 for more information on the peer review process.)

4.5.3 AJM Roles and Responsibilities

A designated Group Manager within AJM must:

- Review and approve the following safety documentation during solution implementation:
  - Sub-System Hazard Analysis (see Appendix F)
  - System Hazard Analysis (see Appendix G)
  - Operating and Support Hazard Analysis (see Appendix H)
- Review and conduct product approval of certain RTCA DO-278A (or equivalent) documentation, as described in Appendix M.
- Provide approval of the system before deployment by deciding if the developer has complied with the performance requirements of the contract.

4.5.4 ATO Chief Safety Engineer Roles and Responsibilities

The primary function of the ATO Chief Safety Engineer is to provide safety leadership and expertise to ensure that:

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

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 certain SRM documentation associated with NAS changes that require AOV approval, as defined in FAA Order 1100.161;
- Review and approve certain SRM documentation for acquisition programs and safety analyses/assessments for changes done at the national level, as defined in the SMS Manual and the SRMGSA;
- Review and approve the following safety input in support of JRC investment decisions and solution implementation, as required:
  - PSP (see Appendix A)
  - OSA (see Appendix C)
  - Comparative Safety Assessment (see Appendix D)
  - Preliminary Hazard Analysis (see Appendix E)
  - System Safety Assessment Report (SSAR) (see Appendix I)
- Provide final safety approval before a system may be deployed to ensure all system safety requirements have been met;

- Serve as the ATO safety focal point for collaboration with ANG and the PO on NextGen transitional activities;
- Ensure that the safety risk case management process includes Integrated Safety Management to ensure a comprehensive safety review of concepts, solutions, systems, and procedures;
- Provide the Director of Policy and Performance, AJI-3, 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 proposed changes to safety policy and guidance for incorporation in FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*, the SMS Manual, and the SRMGSA; and
- Collaborate with internal and external stakeholders to facilitate mitigation of safety risks that cross LOBs.

4.5.5 AJI Roles and Responsibilities

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

4.5.5.1 AJI Safety Engineering Team Manager

For new SRM efforts related to acquisitions and capabilities, the Safety Engineering Team, AJI-314, Manager is the first AJI POC for Program and Portfolio Managers. The AJI-314 Team Manager manages the safety case workload for a team of safety engineers and assigns an AJI SCL to work with an individual program or initiative based on resource availability. He or she ensures that SRM documentation is processed in accordance with the SMS Manual, relevant ATO-SG documents, and the SRMGSA before being submitted to the ATO Chief Safety Engineer for approval and signature.

The AJI-314 Team Manager must:

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

4.5.5.2 AJI SCLs

The AJI SCLs (or their designees) are experts in SRM policy and guidance that pertains to the AMS. The AJI SCLs assist the POs responsible for conducting or managing system safety programs. The AJI SCLs are the ATO's acquisition safety focal points and ensure that each safety product associated with an AMS milestone is peer reviewed; they ensure that all resulting

comments and concerns are addressed prior to the program's planned AMS decision. The AJI SCLs must:

- Meet with the POs and convene 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 PO, when assigned by the AJI-314 Team Manager, to guide the team in conducting and developing the safety analyses and the PSP. As the SRM documentation is being developed, the AJI SCLs provide periodic feedback to the PST. At the appropriate time, they recommend to the AJI-314 Team Manager that the SRM documentation is ready to enter the peer review process for approval and signatures.
- Coordinate the peer review of SRM documentation with the PO (see Section 8.4) within a timeframe 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 ANG or SCT-chartered teams as requested to represent the entire ATO from a safety perspective.
- Ensure that safety risks associated with initiatives that have conducted safety analyses/assessments are mapped to and considered in the SRM activities of any acquisition program.
- Identify, evaluate, and document lessons learned.

4.5.5.3 AJI Audits and Assessments Group

The Audits and Assessments Group, AJI-32, provides the ATO with mechanisms to ensure the safety of the NAS by identifying areas of risk or concern. The group uses a streamlined process to audit requirement compliance and assess the effectiveness of mitigation strategies. The group also uses a structured process to assess the safety and operational readiness of new systems prior to deployment in the NAS.

The Independent Safety Assessments Team, AJI-321, is responsible for evaluating designated acquisition systems (and major modifications) through the Independent Operational Assessment (IOA) function.[11] To ensure that solutions are within acceptable levels of safety risk, the SMS and the AMS require that IOAs be conducted on designated systems prior to the deployment decisions (such as the In-Service Decision (ISD)) to identify safety hazards and operational concerns in a representative operational environment.

AJI-32 will perform RTCA DO-278A compliance spot audits to support the signing of the SSAR by the ATO Chief Safety Engineer.

During the ISM phase, AJI-321 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.

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

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

4.5.5.4 ISD Executive Secretariat

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

5 Safety Planning for Acquisitions

5.1 Portfolio Safety Strategy

The Next Generation Air Transportation System (NextGen) Investment Portfolio Leads are responsible for ensuring the conduct of Integrated Safety Management within their portfolio. This is not an independent effort; the Office of NextGen (ANG) needs to rely on the input of Safety and Technical Training (AJI) to fully assess the safety posture of any portfolio and to plan Integrated Safety Management efforts. At a high level, AJI supports ANG and NextGen Integrated Safety Management by participating in safety assessments and Safety Collaboration Team (SCT)–directed safety analyses, as requested. AJI also provides consolidated Air Traffic Organization (ATO) safety reviews of NextGen planning documents.

AJI support also includes:

- Collaborating with ANG on all aspects of NextGen Integrated Safety Management to ensure that safety artifacts are developed as needed during the pre-investment phases of the Federal Aviation Administration Acquisition Management System (AMS);[1]
- Developing a single ATO safety strategy to support NextGen concepts and implementation as depicted on the National Airspace System Enterprise Architecture (EA) safety roadmap as well as tracking ATO Safety Decision Points on the EA safety roadmap;
- Approving the scope of NextGen safety assessments conducted in the pre-investment phase;
- Participating in safety assessments and SCT-directed safety analyses, as requested;
- Reviewing and approving Safety Risk Management (SRM) documents for NextGen solutions;
- Reviewing and approving safety operational improvements' functionality and implementation dates in the NextGen Safety Portfolio; and
- Attending technical meetings between ANG and Program Offices (POs) to coordinate safety program requirements and engineering architecture artifacts.

In addition, AJI and the PO work with the ANG NextGen Investment Portfolio leads to identify any Integrated Safety Management gaps that may exist within a portfolio.

5.2 Safety Strategy Meetings and Program Safety Plans

Acquisition strategies vary among investment programs. As a result, the SRM documentation requirements may also vary. The PO should contact AJI to schedule a Safety Strategy Meeting (SSM) to determine the appropriate documentation requirements and to receive guidance in fulfilling the PO's SRM obligations for the anticipated AMS milestone. The AJI Safety Case Lead (SCL) facilitates the SSM, contributes his or her knowledge of policies and SRM practices, establishes peer review process guidelines, and ensures that the proceedings are captured in meeting minutes. The SSM should be conducted in consultation with the ATO Chief Safety Engineer, if necessary (particularly if extensive documentation tailoring is planned).

The SSM can be held at any time per the request of the PO from project inception through the fielding of the system (including prior to the Initial Operating Capability being declared).

1. The ANG thrust is prior to the Concept and Requirements Definition and the Initial Investment Analysis phases of the AMS process.

However, to gain the maximum benefit for the program, the SSM should occur early enough in the process to schedule SRM documentation development, review, coordination, and necessary approvals prior to the PO's next investment milestone decision point. SRM is a required checklist item for the Investment Analysis Readiness Decision (IARD), the Initial Investment Decision (IID), the Final Investment Decision, and the In-Service Decision.

In addition to the overall safety strategy, the Program Safety Plan (PSP) and any other SRM products (e.g., Operational Safety Assessment and Comparative Safety Assessment) may be discussed. For each SSM, AJI must prepare meeting notes documenting the strategy agreed upon by attendees to satisfy acquisition SRM requirements. The Enterprise Safety and Information Security Division, ANG-B3, should be invited to participate in all SSMs. For SSMs held for programs in or about to enter the Concept and Requirements Definition (CRD) phase, the POs must consult with the ANG CRD lead before the SSM convenes. The SSM discussion must also include the ramifications of implementing Appendices J, K, L, and M of the Safety Risk Management Guidance for System Acquisitions (SRMGSA) and any requirements that need to be included in the PSP.

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

The PO must use the results of the SSM to develop a program-specific PSP, which must be approved by the ATO Chief Safety Engineer. A PSP must be approved before the IARD, if feasible, but no later than the IID. The PSP defines which safety analyses/assessments must be conducted during a system acquisition and which safety requirements must be fulfilled before system deployment. If documented in an approved PSP, the PO may use alternative methods other than those described in the SRMGSA's appendices to capture required information. Also, if documented in an approved PSP, the PO may prepare a combined analysis (i.e., a combined System Hazard Analysis / Sub-System Hazard Analysis) or bypass analyses entirely to meet AMS requirements.

5.2.1 Consistency with the Implementation Strategy and Planning Document

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

5.2.2 Technology Refreshment Portfolio

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

6 Other Considerations

6.1 Baseline Change Management

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

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

- If the program cost is being re-baselined, the proposed new budget may not include funding to implement the mitigations previously identified.
- If the schedule is being re-baselined, the proposed new schedule may impact the temporal aspects of the identified risk mitigation strategy. 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 from the assumptions made. Analyses conducted as part of previous safety assessments may no longer apply, invalidating previously identified risk mitigation strategies.

6.2 Program Safety Requirements for Decommissioning and Disposal

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

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

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

6.3 Managing Software Risk

Analyzing hazards that are introduced 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. Some of the unique characteristics of software include:

- Software Development Lifecycle (SDLC) – Software follows a defined lifecycle resulting in robust outcomes. Successive steps of architecture, design, coding, development (changes), Quality Assurance / testing (including logic, flow, load, stress, automation, regression, and union), demonstration (user acceptance), release (with configuration freeze), and "hot fixes"[3] eventually reach an acceptable failure ratio. It is with after-the-fact enhancements and backtracking that field failures often arise.
- Software does not wear out. When software fails, it may be due to a design or implementation defect that has always existed (i.e., a latent defect), a recent enhancement not subject to the full SDLC, or a change in the operating environment that the software was not designed to accommodate.
- Software usually fails without warning. Robust software includes error detection and correction functions to find and fix typical problems using "restores," "restarts," and optimization tools. Abnormal error conditions, unexpected process terminations, and long-duration problems not encountered during testing may still arise. Latent defects, specification errors, and issues with enhancements may have existed before the release of the product and may only be triggered or recognized once many software modules are in broad use under a stressing variety of field operating conditions.
- 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. Reuse of existing code modules helps reduce errors. Device software may also be integrated with Commercial Off-the-Shelf (COTS) system 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. Modular design helps isolate code into independent blocks.
- A line of software code can be easily changed. However, determining the consequences of that change is more difficult.
- Seemingly insignificant changes in one area of software functionality can lead to defects in unrelated areas of functionality.
- Requirements validation is most effective when analysis is performed early in the development of the requirements.
- The AMS requires that the software design be commensurate with the severity of any identified hazard and identifies RTCA[4] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*, as the preferred means to implement that rigor. This requirement spans the AMS lifecycle and includes In-Service Management. Any changes to fielded

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

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

software that is already RTCA DO-278A compliant must maintain RTCA DO-278A compliance. If the original vendor is making the changes, then that vendor must continue to follow their accepted development processes. However, if product maintenance has been transferred to FAA Second-Level Engineering, then that organization must also use an RTCA DO-278A–compliant process when making the change.

6.4 Site Implementation

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

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

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

6.5 Legacy System SRM

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

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

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

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

the Air Traffic Organization (ATO) Safety Management System (SMS) Manual for SRM document requirements.

Changes to legacy systems can involve the addition of new functions or the introduction of a new combination of existing functions to the legacy system. New technologies may also have an effect on existing hazards or how they are controlled. For example, a particular function may be activated by a mechanical switch in the legacy system but enabled by software in the legacy system's changes. If the analysis of the changes determines that there are new or newly combined functions, or if there is any impact on existing hazards or how they are controlled (or any introduction of new hazards), the standard SRM activities documented in the SMS Manual are required.

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

A program undergoing legacy system changes needs to comply with all aspects of the AMS and SRM processes. The requirements for each legacy system change are typically very streamlined or tailored compared to the original program. For legacy system changes, the PO must conduct an SSM (consulting with the ATO Chief Safety Engineer, as necessary) to identify the SRM requirements as soon as practicable. Each legacy system change varies in its purpose and requirements, but the SRM requirements may be minimal if the legacy system change's form, fit, and function are the same as when the program first went through the AMS process.

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

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

6.6.1 Safety and Security Issue Reporting

Regardless of whether an issue falls within the scope of the SMS, the PO is responsible for reporting any potential OSH, information security, operational security, physical security, and cybersecurity issues identified by an SRM panel to the appropriate authority for possible

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

mitigation. Such issues must also be recorded in the SRM document. The appropriate authority for most security issues is System Operations Security. OSH issues (including FLS) should be reported to the appropriate Service Area's OSH/FLS professional or to Environmental and OSH Services headquarters.

6.7 COTS Products

Using a COTS product, even if it has very high reliability, does not imply that the product is safe when it interacts with other system components. Problems could be exacerbated by software because software usually controls many, if not all, of the interactions between system components. Techniques for dealing with COTS by simply equating software reliability or correctness (consistency with specifications) with safety may not prevent system accidents. In many cases, using COTS components in safety-critical systems with acceptable risk may simply be infeasible. In these cases, it is safer and less expensive to provide special-purpose software; using COTS amounts to false economy that costs more in the end.

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

6.8 Safety Performance Targets and Monitoring Plans

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

However, this verification and validation of safety requirements does not eliminate the need for monitoring the safety performance of the fielded system. The PO must establish safety performance targets and begin development of the Safety Requirements Verification Table for all hazards that were identified in the PHA and develop an operational monitoring plan to track these performance targets. The duration of the monitoring activities depends on the complexity of the system being deployed, the sites at which the system will be deployed, and the nature of the established performance targets. The monitoring itself must be conducted by the risk acceptor or his/her designee.

The PO must also recognize that:

- The SSAR may identify workarounds to safety requirements that were not implemented prior to initial deployment, despite the In-Service Decision Authority granting approval to deploy.
- Additional safety requirements may be developed post–Initial Operational Capability as a result of an Operational Suitability Demonstrations, Independent Operational Assessments, or Post-Implementation Reviews.

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

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

6.9 Program Segmentation

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

6.10 Program Risk Management

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

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

Uncontrolled copy when downloaded

7 Equivalent Processes

Every program is different in scope, complexity, criticality, and resources. In recognition of these differences, Program Offices may use other equivalent processes when conducting the hazard analysis portion of Safety Risk Management. An equivalent safety analysis may be used under the following conditions:

- The equivalent process must meet the minimum requirements for a safety analysis outlined in the Air Traffic Organization (ATO) Safety Management System Manual.
- The use of equivalent processes (including alternatives to RTCA[1] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*) must be discussed with and approved by the ATO Chief Safety Engineer and documented at the Safety Strategy Meeting.
- The equivalent process must be described in an approved Program Safety Plan.

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

8 Safety Risk Management Documentation, Approval, and Tracking

8.1 Safety Risk Management Documents[1]

For an acquisition, the system safety process is a series of analyses/assessments that starts at the Operational Safety Assessment (OSA) and the Comparative Safety Assessment (CSA) and continues through the Preliminary Hazard Analysis (PHA), the Sub-System Hazard Analysis (SSHA), the System Hazard Analysis (SHA), the Operating and Support Hazard Analysis (O&SHA), and System Safety Assessment Report (SSAR). Each analysis/assessment becomes more discrete as more design details are known. The basis of each analysis/assessment is a Hazard Analysis Worksheet (HAW).[2] The HAW, initially developed early in the system lifecycle (i.e., in a PHA), is further developed, modified, and enhanced as subsequent analyses/assessments are conducted. Each subsequent analysis/assessment has a slightly different focus but is essentially a HAW in nature that builds on a previously developed HAW.

Thus, the Safety Risk Management (SRM) document becomes a report, or a series of reports, that describes the SRM process that has been conducted with regard to a proposed change or investment. The SRM document records the safety risk analyses/assessments that were performed and the findings that detail the predicted risk level(s) of the proposed change or investment. It is a compilation of the SRM documentation completed to date. As such, the SRM document expands with each analysis/assessment as a product moves through the Federal Aviation Administration (FAA) Acquisition Management System (AMS) lifecycle. When it is determined at the Safety Strategy Meeting (SSM) that specific safety analyses/assessments are required, the analyses/assessments are documented and become part of the SRM document. Each Program Office (PO) must maintain an SRM document as a record of the progress of the project.

In colloquial terms, imagine a folder titled “SRM document for Acquisition XXX.” Every analysis/assessment performed for this acquisition is titled “SRM document – (analysis/assessment name here)” and stored in the folder. Each analysis/assessment is an SRM document, but the entire folder is the SRM document for the acquisition. In conversation, especially when a milestone is approaching, questions may be raised about the status of the SRM document; in most cases, the requestor is concerned about the status of the most recent analysis/assessment rather than the entire folder.

For safety documents required to be approved before a particular acquisition milestone decision point, the PO must record SRM document activity and information in the Safety Management Tracking System (SMTS) prior to that milestone. For other SRM documents (e.g., the SHA, SSHA, and O&SHA), SRM document activity and information must be recorded in SMTS within 30 days after document approval. (See Section 8.5 for details on what must be uploaded.) The PO must also upload a copy of the approved Program Safety Plan (PSP) to SMTS.

If an acquisition change is not expected to introduce new hazards or increase safety risk into the National Airspace System (NAS), then there is no need to conduct further safety analyses; however, the PO must document this determination in an SRM document along with justification

1. Risk acceptance must be obtained for any safety analysis/assessment in which safety risk is identified (except for the OSA and CSA).

2. The HAW is detailed in Appendix E.

as to why the change is not subject to additional SRM assessments. The SRM document must also include a:

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

8.2 Mission Support Programs

When an acquisition has an effect on the safety of the NAS, the PO must conduct and document the SRM process throughout the lifecycle of the product or service in accordance with Air Traffic Organization (ATO) Safety Management System (SMS) policy. In the AMS, Safety and Technical Training (AJI) is designated as the responsible office for determining whether an acquisition affects the safety of the NAS. If AJI has determined that there is no effect on the safety of the NAS (i.e., a Mission Support program), then the ATO Chief Safety Engineer provides documented notification to the Joint Resources Council (JRC) Executive Secretariat accordingly. Program representatives should contact the Safety Engineering Team, AJI-314, Manager to initiate discussions if they believe the program is exempt from SMS requirements. If it is determined that SRM is required for a Mission Support program, then the PO must conduct the program in accordance with appropriate requirements in the ATO SMS Manual / Safety Risk Management Guidance for System Acquisitions (SRMGSA).

8.3 Peer Review Process

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

Acquisition-related SRM documentation requiring ATO Chief Safety Engineer approval (i.e., PSPs, OSAs, CSAs, PHAs, and SSARs) must undergo an AJI-led peer review before being submitted (SRM documents without hazards normally do not undergo the full peer review process). The PO must submit the SRM documentation to the AJI-314 Team Manager, who assigns an AJI Safety Case Lead (SCL) to coordinate the peer review process. The AJI SCL must first review the SRM documentation to determine whether it meets all applicable SRM requirements and guidelines contained in the SMS Manual and the SRMGSA. (If the AJI SCL is the one to submit the SRM documentation for peer review, then this step may have already occurred.) If the AJI SCL determines that the SRM documentation is not ready for a peer review, then he/she returns it to the originator with recommendations for resolution.

The AJI SCL distributes the SRM documentation for peer review and comments according to the guidelines contained in the SRMGSA and internal AJI operating procedures. After comments are received and collated, the AJI SCL works with the PO to generate written responses to the original commenters. The AJI SCL then determines acceptance from the original commenters, recording any discrepancies associated with partial acceptance or non-concurrence. (Acceptance can be determined by a combination of email, phone conversations, and meetings. Meetings are preferred when comments and/or responses are complex.) The AJI SCL will then provide a final compilation of all comments and their dispositions to all reviewers. The PO is responsible for updating the SRM documentation in accordance with the adjudicated comments.

Figure 8.1 shows a high-level flow diagram of the entire document review process, of which the peer review process is a subset.

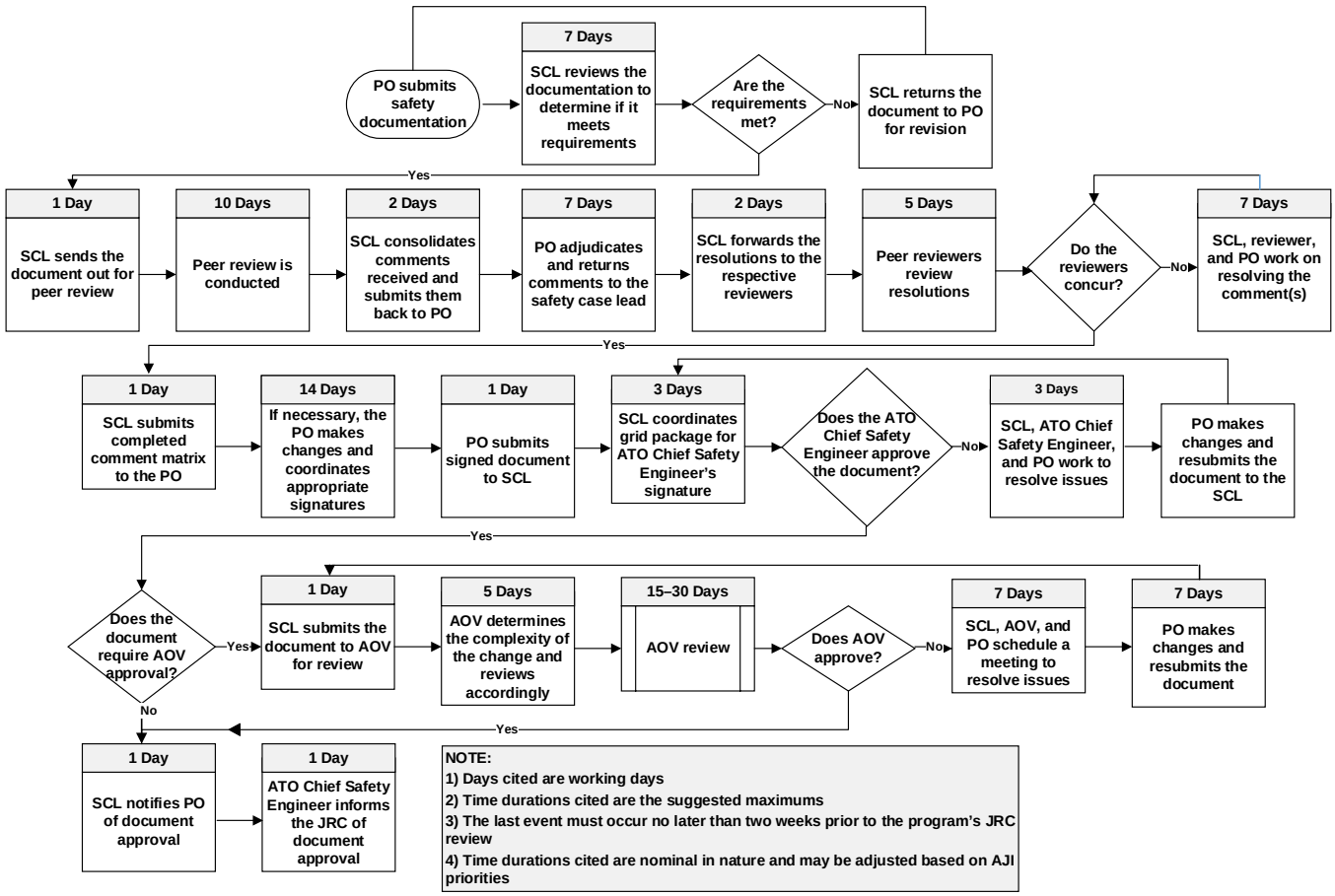

Figure 8.1: Document Review Process Flow

Peer reviewers are designated as either primary or secondary reviewers depending on their role in the approval process and by the guidelines listed below.

Primary reviewers include:

- Other AJI SCLs;
- Other AJI representatives;
- Independent Safety Assessments Team, AJI-321, representatives;
- The Office of NextGen (ANG) Enterprise Safety and Information Security, ANG-B3, representatives;
- Representatives from offices responsible for implementing safety requirements (e.g., Aircraft Certification Service); and
- Representatives from offices responsible for accepting safety risk.

Secondary reviewers, as required, include:

- Quality Control Group representatives from the Service Center,
- Air Traffic Safety Oversight Services (AOV) Air Traffic Safety Standards Oversight, AOV-100, representatives,
- Human Factors representatives,
- Environmental and Occupational Safety and Health Services representatives,
- Cybersecurity representatives, and
- Representatives from other AJI offices.

The peer review timeline is dependent upon various factors including, but not limited to, the complexity of the safety analysis/assessment, the number of stakeholders involved, new technologies involved, prior reviews, and projected JRC decision dates. The AJI SCL negotiates with the PO for firm review dates, if possible, during the initial SSM. Timelines can be reduced if draft versions have been already reviewed. If comments cannot be resolved to the satisfaction of the original commenter, then the AJI SCL identifies them as issues for inclusion in the final briefing package provided to the ATO Chief Safety Engineer upon recommendation for approval by the AJI-314 Team Manager.

Per Section 2.2.2, the Program Management Organization (AJM) must approve the following safety deliverables as required by the contract: the SHA, the SSHA, and the O&SHA (or the SAE Aerospace Recommended Practice (ARP)[3] ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*, equivalents). Similarly, AJM must approve the following safety deliverables related to RTCA[4] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*: the Plan for Software Aspects of Approval, the final Software Configuration Index, the Software Accomplishments Summary, and any other related deliverables as required by the contract. Prior to AJM approval of a safety deliverable, the individual PO must send the safety deliverable to the AJI SCL to conduct a review and make any comments by the requested due date. The PO must also ensure that the safety deliverable is peer reviewed by appropriate subject matter experts. The PO must review and adjudicate the AJI SCL comments in parallel with the comments received during the peer review. After the AJM peer review process is completed and all comments are adjudicated, the safety deliverable may be finalized, approved, and signed in accordance with AJM procedures.

8.4 Approval Authorities and Coordination Requirements

The SMS Manual contains the guidance and coordination requirements for the review, approval, and risk acceptance of SRM documentation contained completely within a Service Unit (SU), across multiple SUs, or across multiple lines of business. SRM documentation may not be submitted to the ATO Chief Safety Engineer for approval until after it has undergone the AJI peer review process. However, SRM documents without hazards for an acquisition program that will undergo an Independent Operational Assessment must be submitted to AJI-321 for peer review. The ATO Chief Safety Engineer is also the approval authority for PSPs as well as

3. An ARP is a guideline from SAE International.

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

the representative that informs the JRC and In-Service Decision Executive Secretariat's groups which programs are compliant with SMS requirements.

SRM document signature requirements are provided in the SMS Manual.

8.5 SMTS

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

Listed below are the details required in SMTS:

- Project title (this must be the same program name used for JRC purposes);
- Safety analysis/assessment type (i.e., OSA, CSA, PHA, SHA, SSHA, O&SHA, or SSAR);
- Organization name;
- Organization description (this must be the name of the responsible PO);
- Safety analysis/assessment title;
- Whether the ATO Chief Safety Engineer's signature is required;
- Whether issues/hazards were identified;
- A HAW for each identified hazard (this must include a hazard ID and hazard description). This must be done by the time of implementation (i.e., as part of the SSAR);
- Uploaded copies of the approved PSP; and
- Uploaded copies of the final approved and signed safety analyses/assessment (i.e., OSA, CSA, PHA, SHA, SSHA, O&SHA, SSAR, or other).

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

9 System Safety Considerations

9.1 System Safety

System safety is a standardized management and engineering discipline that integrates the consideration of human, machine, and environment in planning; designing; testing; and maintaining operations, procedures, and acquisition projects. System safety is applied throughout a system's lifecycle to achieve an acceptable level of safety risk within the constraints of operational effectiveness, time, and cost.

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

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

9.2 Integrated Safety Management

The highly distributed and interconnected nature of the National Airspace System (NAS)—and Next Generation Air Transportation System (NextGen), in particular—presents complex safety challenges to the NAS. In addition, many changes to the NAS necessary for implementing 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 the planned interactions and interconnectivity.

The legacy NAS is a "system of systems" that provides multiple services to users. 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 also build on one another, subsume each other, or combine for a joint function or capability. This perspective was not considered historically but is important to applying the concept of integrated safety in acquisitions. Integrated Safety Management must be performed to assess risks of initiatives in support of agency Risk-Based Decision Making.

1. An ARP is a guideline from SAE International.

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

Integrated Safety Management represents a more robust, holistic, and integrated approach to performing safety analyses. It uses existing safety policy and methodologies as well as Systems Engineering processes. It is a critical component not only for successfully achieving the NextGen vision, but also for implementing all enhancements to the NAS.

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

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

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

9.3 FAA / System Developer Interface

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

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

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

- The timing of safety analyses must be consistent with the engineering milestones outlined in the FAA Systems Engineering Manual (see Table 9.1).

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

Table 9.1: FAA System Development / Decision Milestones

Milestone Description	AMS Phase
Concept and Requirements Definition Readiness Decision	**Service Analysis and Strategic Planning***
Functional Hazard Assessment (FHA) conducted	**Concept and Requirements Definition**
Safety requirements (from the FHA, Safety Collaboration Team–sanctioned analyses, and other sources) defined	
Preliminary PRD approved	
Initial Investment Analysis Plan (IAP) approved	
PSP prepared and approved	
Operational Safety Assessment (OSA) conducted and approved	
Safety Requirements Verification Table (SRVT) tracking began	
IARD	
Operational Capability Demonstration completed**	
Additional safety requirements (from the OSA) defined	**Initial Investment Analysis**
Safety input provided in the Program Management Plan (PMP), Implementation Strategy and Planning Document (ISPD), IAP, and preliminary Test and Evaluation Master Plan (TEMP)	
PSP updated	
Comparative Safety Assessment (CSA) prepared and approved	
Additional safety requirements (from the CSA) defined	
PRD update approved	
Preliminary Business Case Analysis approved	
Final IAP approved	
IID	
Updated safety input to the PMP, the ISPD, and the initial TEMP provided	**Final Investment Analysis**
PSP updated	
DIDs for safety analyses, the SSPP, and software development deliverables identified (including contractual language ensuring government involvement in developer-led SRM panels and early government approval of the Plan for Software Aspects of Approval (PSAA)	
System contract specification approved	
Screening Information Request released	

Milestone Description	AMS Phase
In-Service Review Checklist completed	
Preliminary Hazard Analysis (PHA) prepared and approved	
Additional safety requirements (from the PHA) defined	
Safety input to Post-Implementation Review (PIR) Strategy provided	
Final PRD approval	
Final business case approval	
ISPD approval	
Final Acquisition Program Baseline approval	
FID	
Integrated Baseline Review completed	**Solution Implementation**
Contract award	
Systems Requirements Review completed	
Developer-generated SSPP delivered for government review	
Preliminary PSAA submitted for government review	
AJI Audits***	
System Design Review completed	
System Specification Review completed	
Sub-System Hazard Analysis prepared and approved	
Final PSAA submitted for government approval	
Preliminary Design Review completed	
Software Configuration Index submitted for government review****	
System Hazard Analysis prepared and approved	
Critical Design Review completed	
Generic Site Implementation Plan developed	
Product Demonstration Decision	
Provisioning technical documentation delivered	
Factory Acceptance Testing completed	
Safety input to the final TEMP provided	
System delivered to test and evaluation site	
Test Readiness Review completed	
Development Test completed	
NAS Change Proposal approved	
Operational Test completed	
Functional Configuration Audit completed	
Physical Configuration Audit completed	
Software Configuration Index submitted for government approval****	
Production Readiness Review completed	
Draft Software Accomplishment Summary prepared and submitted for government comment	
Production Decision	
Operating & Support Hazard Analysis prepared and approved	
Operator/maintenance training begins	

Milestone Description	AMS Phase
First-site preparation completed	
First-site delivery	
First-site training material delivery	
Government acceptance	
Site-Acceptance Testing completed	
First-Site Initial Operational Capability date	
Independent Operational Assessment (IOA) completed (for designated programs)	
Any new safety hazards from IOA analyzed accordingly	
Safety input to PIR Plan provided	
Software Accomplishment Summary prepared and submitted for government approval	
System Safety Assessment Report (including the SRVT) prepared and approved	
PSP updated for In-Service Management (as necessary)	
In-Service Decision / Initial Operating Capability	
First-Site Operational Readiness date	**In-Service Management**
Full operational capability	
First-site commissioning	
Site Operational Readiness date 25 percent complete	
PIR conducted	
Any new safety hazards analyzed accordingly	
Site Operational Readiness date 50 percent complete	
Site Operational Readiness date 75 percent complete	
Last-Site Operational Readiness date	
Last-site commissioning	

*Not covered by the SRMGSA.

**Indicates the milestone may also be completed during either the Initial or Final Investment Analysis.

***There may be multiple AJI audits conducted during Solution Implementation.

****There may be multiple iterations of the Software Configuration Index (SCI) submitted for approval as the system design matures. The SCI should be updated as necessary with each version of the product and before every formal run of the software test suite.

9.4 Software-Intensive Systems

The PO must demonstrate that software-intensive[3] systems were developed at an appropriate level of rigor. The PO must establish a development assurance program in accordance with RTCA DO-278A and document it in the PSP.[4] In addition, RTCA DO-330, *Software Tool*

3. A software-intensive system is any system where software influences—to a large extent—the design, construction, deployment, and evolution of the system as a whole.

4. This is one acceptable means of demonstrating this level of rigor. Subject to approval by the Program Management Organization, a developer's internal procedures may also suffice.

Qualification Considerations, through RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*, must also be evaluated where applicable; and the approval authority must define the usage guidance of these requirements. Refer to Appendix M for an overview of the required RTCA DO-278A deliverables.

9.4.1 System Development Assurance

When complexity of design increases, the difficulty in preventing errors also increases. Each architectural and technological choice must be evaluated to determine if traditional verification methods will be adequate or if development assurance needs to be applied. Some of the standards used in aerospace to accomplish this include the latest versions of:

- SAE ARP4754A;
- SAE ARP4761A, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*;
- RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*;
- RTCA DO-278A; and
- RTCA DO-254A.

System development assurance is the use of a systematic approach to prevent errors from getting into the design, be it at the enterprise, system, architecture, hardware, or software level. The FAA Acquisition Management System (AMS) process is itself a high-level development assurance activity. In addition to the AMS, SRMGSA, and SMS Manual, the ATO has specifically chosen to use RTCA DO-278A and supporting supplements, RTCA DO-330 through RTCA DO-333, to accomplish development assurance for acquired software. The PO has the discretion to decide which standards to use for other aspects of development assurance for its systems. (Those listed above are recommended.) Development assurance extends throughout the entire product lifecycle.

9.4.1.1 Determining the Development Assurance Level

Risk analysis is performed to determine the proper level of rigor to be applied during design, development, and testing. An appropriate level of rigor is necessary to ensure confidence that the component does not cause or contribute to a system hazard. Determining the Development Assurance Level (DAL) related to a hazard is a three-step process:

1) Determine a hazard's severity classification based on the expected effects of the hazard. Refer to the severity classifications defined in RTCA DO-278A, Section 2. (*Note*: These severity classifications may be different from those in the SMS Manual.)
2) Assign the DAL in accordance with the hazard's severity classification within a given function/component. (There may be more than one DAL within a system due to partitioning.)
3) Determine whether architectural considerations warrant a DAL different from the initial DAL. In some cases, architectural mitigation may justify a revision of the DAL to a less stringent classification. Guidance for architectural mitigation can be found in SAE ARP4754.

Software that can be a causal factor for hazards must be evaluated to determine the appropriate DAL per RTCA DO-278A. The DAL is the mitigation that prevents the hazard of a

developmental error. Compliance to a DAL is a safety requirement that must be identified in the SRM document in order for it to be properly tracked and eventually verified and validated. 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. System and hardware DALs are determined using SAE ARP4754 and RTCA DO-254. Appendix J provides more detail on determining the correct DAL.

9.4.1.2 RTCA DO-278A Compliance Gap Analysis

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

The PO must conduct an RTCA DO-278A compliance gap analysis for each function within the system/software being evaluated. RTCA DO-278A guidelines ensure a specific software design and development assurance from the system's safety analysis process, one that is based on software architecture and functions. The RTCA DO-278A compliance gap analysis provides a basis for addressing any shortfalls from the required RTCA DO-278A objectives. The gap analysis compares existing processes with RTCA DO-278A and identifies deficiencies. The process is then improved to resolve the deficiencies.

The PO must describe the improved process in the PSAA, which is provided to the approval authority along with the RTCA DO-278A compliance gap analysis. This PSAA not only defines the PO's/vendor's plan for RTCA DO-278A compliance but also documents the deficiencies found in the gap analysis as well as the plan to resolve these gaps. The PSAA must be summarized or referenced in the PSP.

Conducting the RTCA DO-278A compliance gap analysis is not a specific safety responsibility. Typically, this effort is led by the PO acquiring the new system or proposing changes to an existing system. This is typically done with help from the prime contractor conducting systems integration and the subcontractor(s) responsible for developing the software. Ideally, it should be performed before the contract award as a way to evaluate different vendors. Other key participants in the process are the approval authority and the RTCA DO-278A SME (someone who has qualified skills and knowledge related to software assurance, specifically related to RTCA DO-278A or RTCA DO-178C, and who is acceptable to the approval authority). Appendix K provides more detail on developing an RTCA DO-278A compliance gap analysis.

9.4.1.3 Software Approval Process

The software SME within the PO must review the software lifecycle processes and associated data to confirm that a software product complies with the approval basis and RTCA DO-278A. The PO should involve the AJI safety case lead in this review, as appropriate. The software review process assists the applicant, approval authority, and system developer in determining whether a project meets the approval basis and satisfies RTCA DO-278A guidance. The software review process does this by providing:

- Timely technical interpretation of the approval basis, RTCA DO-278A guidance, approval authority policy, issue papers, and other applicable approval requirements;
- Visibility into the methodologies being used to comply with the requirements and supporting data;
- Objective evidence that the software project adheres to its approved software plans and procedures; and
- The opportunity for the approval authority to monitor SME activities.

The Program Management Organization (AJM) must approve the PSAA, the Software Configuration Index, and the Software Accomplishment Summary (see Appendix M). Lifecycle data items are described in RTCA DO-278A, Section 11. Appendix L provides more detail on the software approval process. Evidence of the AJM review must be submitted to the ATO Chief Safety Engineer so he/she can conduct the safety approval process.

Appendix A

Guidance for Preparing and Implementing Program Safety Plans

Guidance for Preparing and Implementing Program Safety Plans

1 Purpose

This guidance outlines a process consistent with the Air Traffic Organization (ATO) Safety Management System (SMS) for preparing and implementing Program Safety Plans (PSPs) for systems that may be fielded in the National Airspace System (NAS) and that are 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, which provides guidance on fulfilling requirements set forth in the current version of FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements the AMS.

3 Background

A PSP is the government's integrated management plan for conducting the System Safety Program (SSP) for a particular project or program. By executing this plan, the government ensures compliance with the provisions of the SMS Manual, the Safety Risk Management Guidance for System Acquisitions (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.

The Program Office (PO)[1] (using a Program Safety Team, as appropriate) 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 System Safety Program Plan (SSPP), which is typically required as a contract deliverable. The prime contractor's SSPP, when approved by the government, binds the contractor to an SSP that should be consistent with the government's PSP.

The PSP also stands as the PO's agreement with Safety and Technical Training (AJI) (or more specifically, the ATO Chief Safety Engineer) to conduct a safety program that is consistent and compliant with the ATO SMS. It defines the roles and responsibilities of the PO / Safety Team members as they implement the SSP. As such, the PSP must describe:

- The safety program that applies to each project, sub-system, and interface to support program activities and SMS/SRM requirements;
- The SRM responsibilities of the PO / Safety Team;
- Planned SRM efforts; and
- A summary of the development assurance program (either as proposed or as documented in the program's Plan for Software Aspects of Approval (PSAA)).

4 System Safety Considerations

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

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

PSP. In addition, the timing of the required safety analyses must be consistent with the engineering milestones outlined in the FAA Systems Engineering Manual (SEM). A Data Item Description (DID) describes the SSPP requirements to be placed on contract. (DIDs are available in the DID Library.) These DIDs may be tailored by the PO as necessary. The specific delivery timeframes and review processes for each DID must be included in the Contract Data Requirements List.

In addition:

- Any SRM panel facilitated or conducted by the developer (i.e., to develop a Sub-System Hazard Analysis or a System Hazard Analysis) must include Subject Matter Experts (SMEs), particularly those with an operational perspective. This must be reflected in both the PSP and the SSPP and within the developer's contract.
- The government must actively review and be able to modify/comment upon the safety analysis documentation as it is being prepared by the developer (i.e., not just at its final delivery). This must be reflected in both the PSP and the SSPP and within the developer's contract.
- An AJI-approved PSP must be in place prior to any Joint Resources Council (JRC) milestone decision or In-Service Decision (ISD), per AMS policy. As system functionality is often operationally released in segments or phases, there may be multiple ISDs for an acquisition or modification to an existing NAS system. The PSP to support the Final Investment Decision (FID) must discuss ISD strategy (i.e., required number of ISDs) documented in the Implementation Strategy and Planning Document (ISPD)). It is possible that separate PSPs may be required for each segment/phase.
- If the deployment strategy is not well-defined at the FID, the ISD strategy may simply state that the entrance criteria for an ISD (i.e., test, security, safety, and Independent Operational Assessment (IOA)) will be met for each release/phase of the deployment. In this situation, the PSP may need to be updated during Solution Implementation to accurately reflect the final ISD strategy. In addition, if the deployment strategy changes, the JRC requires that the ISPD be updated to incorporate the changes; the PSP may also need to be updated if these changes affect the ISD and/or safety strategy.
- The PSP must reference the version (i.e., the publication date) of the SRMGSA / SMS Manual in effect when the PSP was prepared. Upon PSP approval, the applicable versions of the SRMGSA / SMS Manual will become the operative documents that the PO must follow for the remainder of the program unless the program is restructured via a change in scope, segmentation, or rebaselining. The PO should consult with the AJI Safety Case Lead (SCL) for advice when this has occurred because the approved PSP may no longer apply, and the PSP may have to be updated. The PSP must summarize or reference the PSAA when it is finalized.

5 Procedures

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

1) Identify the SSP requirements;
2) Develop a safety strategy based on these requirements;
3) Translate the developed safety strategy into a PSP;
4) Submit the PSP for approval and signature;
5) Implement the SSP in accordance with the PSP;

6) Update the PSP, as needed; and
7) Monitor and review the progress of PSP implementation.

5.1 Identify the SSP Requirements

Requirements identification is an initial step that must be conducted to tailor a program's safety strategy. The PO, the Safety Team, the AJI SCL, the Office of NextGen, and other stakeholders collaborate to identify the requirements and solidify them via one or more Safety Strategy Meetings (SSMs). The AJI SCL may also recommend language to be included in any contracts to enhance the government-developer system safety interface. The identification process consists of several sub-steps, as documented below.

5.1.1 Review Generic System Safety / SMS and AMS Program Requirements

The PO / Safety Team should review generic source documentation such as the AMS (specifically Section 4.12, *National Airspace System Safety Management System*), the SMS Manual, the SRMGSA, and applicable FAA orders (such as FAA Order JO 1000.37 and FAA 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.

5.1.2 Identify Mechanism for Tracking and Monitoring Program Hazards

FAA Order JO 1000.37 requires that all identified safety hazards and their safety risks be recorded in a database. The PO / Safety Team must use the Safety Management Tracking System (SMTS) to enter data for new safety analyses before beginning the monitoring process. Enter all hazards into SMTS, including those with low risk. The PO / Safety Team must ensure that personnel have been trained to use this system and that SMTS use is integrated into the SSP. (Refer to Section 8.5 of the SRMGSA for further information regarding SMTS.)

5.1.3 Identify Developmental Assurance Requirements

Each architecture and technology choice must be evaluated to determine if traditional verification methods will be adequate or if developmental assurance requirements need to be applied. Development assurance is typically required for complex systems whose anomalous behavior can cause or contribute to a failure condition with safety-related consequences. Complexity of both hardware and software is a hazard cause and may or may not be a contributor to the hazard under consideration.

The PSP must include a discussion of:

- System development assurance,
- Hardware development assurance, and
- Software development assurance.

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

It is highly recommended that software development assurance be conducted in accordance with RTCA[2] DO-278A, *Software Integrity Assurance Considerations for Communication,*

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

Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems.[3] Since the Assurance Level (AL) can have an 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. Review SRMGSA Appendices J, K, L, and M for further development assurance requirements and information.

The following topics must be addressed in the PSP:

- The activities the vendor's Software Quality Assurance (SQA) will conduct on the development to ensure compliance with RTCA DO-278A.
- The activities the PO will conduct on the vendor SQA's oversight activities.
- The activities the PO will conduct on the vendor's development to validate compliance with RTCA DO-278A.
- The Program Management Organization's process for approving vendor-submitted RTCA DO-278A documents.

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

5.1.4 Identify Initial Operating Capability Safety Requirements

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

5.1.5 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 whether the program is achieving expected performance targets (including those resulting from safety requirements) and meeting the service needs of the customers. The PIR seeks to validate the original program business case. The PIR also seeks to provide lessons learned with regard to the original program business case for application on future business cases. A PIR strategy is developed in the AMS lifecycle during the Final Investment Analysis and must include appropriate safety considerations, which should be incorporated into the PSP.

For acquisition programs, monitoring responsibilities end when all activities outlined in the SRM document monitoring plan and the safety section of the PIR Plan are complete. After the ISD, additional safety requirements may be identified via a PIR or other means that could result in design changes to the system.

3. Other acceptable alternatives to RTCA DO-278A exist for conducting software development assurance. Alternative guidance can be used with approval from the ATO Chief Safety Engineer.

5.1.6 Develop a Nominal Safety Program Schedule

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

5.1.7 Perform an SRMGSA Compliance Review

The PO must review the PSP periodically and update it to ensure all the requirements identified in the SRMGSA are accounted for and sufficient details exist in the plan for execution.

5.2 Develop a Safety Strategy Based on Identified Program Requirements

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

5.2.1 Prepare a Safety Strategy Worksheet

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

- System/program name and previous program name, if any;
- Short system description;
- System/FAA/external interface(s);
- Interdependencies;
- Changes to legacy systems, if any;
- Name / phone number of key individuals: PO, leader of the Safety Team, AJI SCL, applicable Service Unit SMEs, and RTCA DO-278A SME;[4]
- Where the program is in the AMS lifecycle;
- Any plan for combining JRC decision points;
- Whether alternative solutions may be proposed;
- Proposed dates of the JRC investment decisions and IOC/ISD;
- Impact of the system on the NAS, separation, navigation, communications, and aircraft;
- A listing of any safety assessments completed to date and a summary of any safety findings, including potential safety risk impacts of the system on the NAS;

4. An RTCA DO-178 Designated Engineering Representative would be considered an RTCA DO-278A SME.

- Traceability to a Next Generation Air Transportation System (NextGen) portfolio, including any requirements allocated from the portfolio;
- Traceability to NAS Enterprise Architecture (EA) elements (e.g., systems, functions, operational activities, information exchanges, data exchanges). This may be provided in the form of previously delivered program-level NAS EA products;
- Traceability to any previously conducted AJI SCL-authorized analyses and assessments that impact the program; and
- IOA designation, if applicable.

5.2.2 Organize and Hold the First SSM

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

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

The outcome of this meeting is a safety strategy that is mutually agreed upon by the PO, the AJI SCL, and other stakeholders.

5.3 Translate the Safety Strategy into the PSP

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

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

- Hazard analyses to be performed;
- Processes for using SMTS;
- Potential safety performance metrics, including safety performance indicators, initial baseline values, and residual target values (safety data to be collected, including metrics, baseline values, safety performance indicators, and target values);
- Safety requirements management;[5]
- Safety assessment review plan (i.e., the type of safety assessment program to be used and scheduled for accomplishing safety verification and validation);
- Safety management of program changes (e.g., scope, design, schedule);
- Safety training required;
- Development assurance considerations (e.g., RTCA DO-278A applicability, AL considerations, architectural mitigation);
- Safety interfaces with development engineering, support contractors (pre-FID), prime contractors (post-FID), management, and other specialty engineering groups;
- Dependencies on other PSPs; and
- IOA designation with justification, if applicable.

5.4 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 PO for approval.
- If acceptable, the PO 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 SCL for coordination, approval, and signature by the ATO Chief Safety Engineer.

5.5 Implement the SSP in Accordance with the PSP

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

5.6 Update the PSP as Needed

The PSP is a living document that must be updated by the PO as circumstances change (e.g., different acquisition phases, changes to the program structure/management team, program financial profile, program approach). The initial PSP, at either the IARD or the IID, may be based only on the high-level safety objectives developed in the Operational Safety Assessment. At this stage, the PSP should at least acknowledge that—depending on the architectural implementation of the operational solution—there may be further allocation of safety requirements to the system as it matures (i.e., RTCA DO-278A may come into play). The later

5. 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.

PSP at the FID should reflect the safety requirements that are in the final Program Requirements Document along with the required verification means. The PSP must be reviewed prior to each AMS investment decision and before IOC or ISD is declared. If agreements made in the original PSP need to be amended, the AJI SCL must resubmit the revised PSP to the ATO Chief Safety Engineer for approval.

5.7 Monitor and Review the Progress of PSP Implementation

The PO must ensure that the PSP is implemented per the agreed-upon schedule (which is subject to revision under certain circumstances) and must inform the AJI SCL of any deviations from the plan. The PO must ensure status inputs are entered into SMTS to enhance AJI's ability to monitor the safety program. The AJI SCL must also monitor the safety program on a regular basis, particularly as JRC milestones approach and as certain required documentation must be approved.

6 Technology Refreshment Portfolio

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

Appendix B

Description and Overview of the System Safety Program Plan

Description and Overview of the System Safety Program Plan

1 Purpose

This guidance provides a description and overview of the System Safety Program Plan (SSPP), which is a document generated by the system developer (contractor) and required and approved by the Program Office (PO).

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the Air Traffic Organization Safety Management System (SMS) Manual, which provides guidance on fulfilling requirements set forth in the current version of FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements the FAA Acquisition Management System (AMS).

The primary reference materials in this guidance are the current editions of the following:

- AMS, Section 4.12, *National Airspace System Safety Management System*
- SMS Manual
- FAA Order JO 1000.37

While the system developer may be contractually obligated to comply with the aforementioned policy documents, additional guidance regarding National Airspace System (NAS) systems engineering processes referred to herein may be found in the FAA Systems Engineering Manual.

3 Overview

An approved SSPP is a contractually binding understanding between the FAA and the contractor regarding how the contractor will meet contractually required system safety requirements.

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

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

4 Purpose of the SSPP

The SSPP accomplishes the following:

- Contains the scope, contractor organization, program milestones, safety requirements, safety data, safety verification, accident reporting, and safety program interfaces;
- Describes the contractor's plan for the implementation of safety requirements;

- Identifies the hazard analysis and safety risk assessment processes that the contractor will use;
- Defines how the contractor will record hazards and predicted residual risk levels and how they will be formally accepted and tracked;
- Provides the FAA an opportunity to review the contractor's scheduling of safety tasks in a timely fashion, permitting corrective action when applicable;
- Provides a milestone prior to beginning software design that is linked to the Plan for Software Aspects of Approval (PSAA) so that safety approval is required before design work can begin; and
- Describes how the contractor will comply with RTCA[1] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems* (or equivalent) and its supporting supplements. (The SSPP should act as the contractor's compliance plan for software development before the PSAA is developed. It should also include the contractor's anticipated PSAA delivery date and an initial estimate of how many Software Configuration Indexes are anticipated to accompany the different software releases.)

5 Establishing the Contractual Requirement

The FAA establishes the contractual requirements for an SSPP in the Statement of Work (SOW). The Data Item Description (DID) for an SSPP (AJI-DID-SSPP) outlines the contents to be included in the SSPP. The PO may tailor the DID accordingly.

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

6 Elements of an Effective SSPP

An effective SSPP clearly details these four elements:

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

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

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

resource allocations for each program element through the term of the contract must also be included.

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

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

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

7 SSPP Contents

The SSPP must detail the following:

- The contractor's program scope,
- Safety organization,
- Program milestones,
- Requirements and criteria[2],
- Hazard analyses,
- Safety data,
- Verification of safety requirements,
- An auditing and monitoring program,
- Training,
- Accident and incident reporting, and
- Interfaces.

7.1 Contractor's Program Scope

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

2. Criteria are principles or standards against which actions may be judged. The government needs this information as it may not know all the internal/external standards that a contractor will be following as part of its system safety program.

7.2 Safety Organization

The SSPP must describe:

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

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

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

7.3 Program Milestones

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

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

7.4 Requirements and Criteria

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

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

7.5 Hazard Analyses

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

7.6 Safety Data

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

7.7 Verification of Safety Requirements

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

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

7.8 Auditing and Monitoring Program

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

7.9 Training

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

7.10 Accident and Incident Reporting

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

7.11 Interfaces

Since conducting an SSP will eventually affect almost every other element of a system development program, a concerted effort must be made to effectively integrate support

activities. Each engineering and management discipline often pursues its own objectives independently, or at best, in coordination only with mainstream program activities such as design engineering and testing. To ensure that the SSP is comprehensive, the contractor must impose requirements on subcontractors and suppliers that are consistent with and contribute to the overall SSP. The SSPP must show the contractor's procedures for accomplishing this task. The prime contractor must evaluate variations and specify clear requirements tailored to the needs of the SSP. Occasionally, the PO procures subsystems or components under separate contracts to be integrated into the overall system.

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

Appendix C

Guidance for Conducting and Documenting an Operational Safety Assessment

Guidance for Conducting and Documenting an Operational Safety Assessment

1 Purpose

This appendix describes the Air Traffic Organization (ATO) Safety Management System (SMS) process for conducting and documenting an Operational Safety Assessment (OSA) of solution concepts.

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the ATO SMS Manual, which provides guidance on fulfilling requirements set forth in the current version of FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements the FAA Acquisition Management System (AMS). Additionally, the systems engineering processes referred to are described in the FAA Systems Engineering Manual (SEM).

The primary reference materials in this guidance are the current editions of the following:

- AMS, Section 4.12, *National Airspace System Safety Management System*
- SMS Manual
- FAA Order JO 1000.37
- FAA SEM
- Safety Management Tracking System (SMTS) User Manual

3 Background

3.1 Description

The Program Office (PO)[1] must conduct an OSA to identify, analyze, and document operational hazards and associated safety requirements early in the AMS planning phases. It is an important part of the FAA's acquisition planning process, especially for the Office of NextGen (ANG), the PO, and the Program Safety Team (PST).[2] The OSA provides early identification and documentation of safety requirements that could improve safety and product integration, lower development costs, and increase product performance and the probability of program success.

An OSA, which may include inputs such as mandated safety analyses or assessments from the Safety Collaboration Team (SCT),[3] is an indispensable tool in allocating safety requirements to lower-level increments.

The PO typically conducts OSAs internally with assistance from the PST and participation from the necessary stakeholders. Some OSAs are international or industry-wide in scope and may

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

2. A PST is a resource provided by the PO to support the safety efforts of the acquisition throughout the AMS lifecycle. As with program management, the leadership and composition of the PST changes as a program proceeds through the AMS lifecycle.

3. The SCT serves as the technical advisory body to the FAA SMS Committee. The SCT's primary function is to facilitate the Integrated Safety Management of pre-decisional NAS changes.

be conducted by industry-wide workgroups chaired by external entities (e.g., RTCA[4]) acting under the guidance of the FAA.

An OSA may be prepared to provide the system designers and management with a set of safety goals for design. The OSA also provides an operational and environmental description and Preliminary Hazard List (PHL) for the proposal and assesses the potential severity of the hazards listed in the PHL. In this phase, the results of any early safety analyses or assessments that affect the program (such as a Functional Hazard Assessment (FHA)) are inputs to the OSA. In addition, certain planning must occur prior to the Investment Analysis Readiness Decision (IARD), such as development of an Investment Analysis Plan, which may require input from the OSA.

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

The PO typically conducts an OSA during the Concept and Requirements Definition (CRD) phase of the AMS lifecycle. CRD activities occur prior to the establishment of clear functions, baseline requirements, alternative solutions, and solution design. An approved OSA is required before the IARD.

3.2 Overview

Figure C.1 shows possible inputs into an OSA, the basic OSA components (the Operational Services and Environment Description (OSED), the Operational Hazard Assessment (OHA), and the Allocation of Safety Objectives and Requirements (ASOR)), and the basic OSA methodology.

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

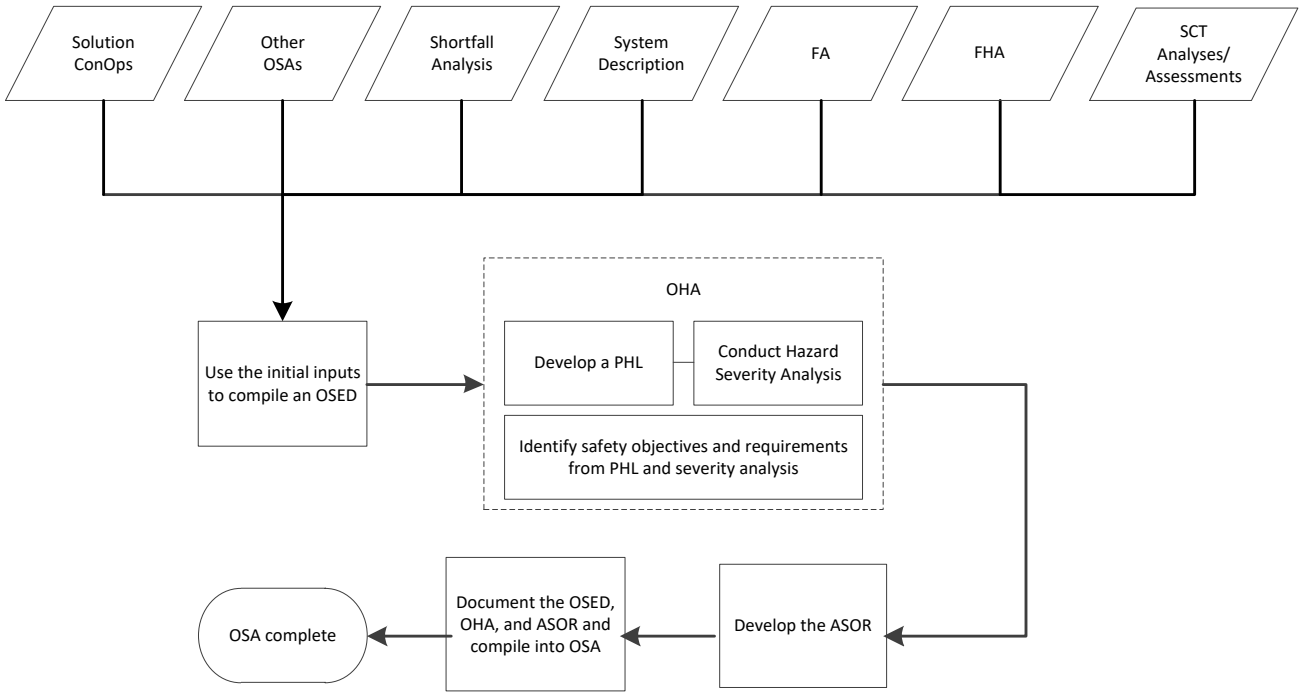

Figure C.1: OSA Inputs, Components, and Methodology

3.3 OSA Components

The OSA components are described in Section 3.3.1 through Section 3.4.3.

3.3.1 OSED

The OSED describes the service characteristics of the solution concept in an operational environment. This description includes both ground and air elements and must include all elements of the 5M Model (as discussed in the SMS Manual). The OSED is used as a mechanism platform to describe the service provided by the solution, the users of the solution, and the varying operational and environmental considerations in which the service is provided for the related Communication, Navigation, and Surveillance (CNS) and Air Traffic Management (ATM) system. The description provided by the OSED is used as a baseline and solution boundary from which to conduct the safety assessment.

3.3.2 OHA

The OHA assesses the operational hazards associated with the shortfall described in the OSED. It determines the severity of each hazard so that operational objectives and safety requirements can be identified for any solution that results in an acceptable level of safety risk when deployed.

3.3.3 ASOR

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

3.4 Use of Results

The results of the OSA are used as input to various documents.

3.4.1 Preliminary Requirements

Controls and safety requirements identified through the OSA process must be included in the preliminary Program Requirements Document (pPRD). The pPRD must include a requirement for DALs in accordance with Appendix J. Other preliminary requirements must be separately documented, such as new/modified Air Traffic Control (ATC) procedures, changes to the Codes of Federal Regulation, and training.

3.4.2 Safety Risk Management Documents

The output of the OSA is used as input for Safety Risk Management (SRM) documents that the PO must develop as the solution is further developed (e.g., Comparative Safety Assessment, Preliminary Hazard Analysis, or System Hazard Analysis / Sub-System Hazard Analysis).

3.4.3 Safety Requirements Verification Table

The Safety Requirements Verification Table contains all of the safety requirements identified, starting with the origin of the requirement (including those identified in the OSA).

4 OSA Inputs

4.1 FHA

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

4.1.1 What is an FHA?

The PO may conduct an FHA to identify credible operational safety effects through the analysis of system or sub-system functions and failure conditions. The FHA is a methodical approach that identifies and classifies the system functions and safety hazards associated with functional failure or malfunction. It identifies the relationships between functions and hazards, thereby identifying the safety-significant functions of the system as well as the hazards associated with that functionality. This identification provides a foundation for the safety program to scope additional safety analyses.

4.1.2 Purpose of an FHA

The purpose of an FHA is to identify every expected function of a system and consider the hazards that may result when each function fails in every possible way. It does not determine causes of the hazards but rather focuses on the consequences and corresponding severities. As a predictive technique, the FHA attempts to explore the effects of functional failures of parts of a system. A guiding principle of the FHA is that if safety requirements are added at the functional level early in the system development process, the design of the system will be more stable from a safety perspective, and the cost of implementing safety mitigations will be reduced.

4.1.3 FHA Overview

The FHA is an engineering-oriented analysis. To conduct an FHA, the PO must convene a technical or engineering-oriented workgroup before any SRM panel is held to review the Functional Analysis (FA), pPRD (if available), Enterprise Architecture (EA) artifacts, and other inputs. To assist the safety program by defining functions and identifying likely functional hazards, the FHA facilitates discussion of mitigations and solutions. The FHA assists any stakeholders participating in subsequent SRM panels (e.g., to conduct OSAs) who may not

have a sufficient technical understanding of the system or change under analysis to fully participate in its functional definition. Subsequent SRM panels must then translate the functional hazard effects into operational effects to assess any operational impacts.

4.1.4 FHA Definitions

4.1.4.1 Function

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

4.1.4.2 FA

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

4.1.4.3 EA Artifacts

EA artifacts include the following:

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

4.1.5 FHA Methodology

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

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

4.1.5.1 FHA Inputs

The following are some of the inputs to an FHA:

- ConOps,
- Operational context description (typically found in the ConOps),
- EA artifacts,

- System architecture data (e.g., inputs, outputs, and flow of functions),
- Policy and standards,
- Interface control documents,
- Legacy system documentation,
- FA,
- pPRD,
- Operational requirements, and
- Maintenance and support concept.

4.1.5.2 FHA Process

Systematically, the FHA identifies:

- The functions, purposes, and behaviors of a system.
- Considerations of how the system fails (e.g., when can the failure conditions occur? In what operational environment will these failures be present?). Consider the following hypothetical failure modes. (*Note*: Additional failure types may be identified through system reports and subject matter expertise.)
    - Fails to operate: Function does not occur/perform when given the appropriate input.
    - Operates early/late: Function performs earlier or later than it should.
    - Operates out of sequence: Function occurs before or after the wrong function; function occurs without receiving the appropriate inputs.
    - Unable to stop operation: Function continues even though the thread should move on to the next function.
    - Degraded function or malfunction: Function does not finish or only partially completes; function generates improper output.
- Impact or effects that failures may have (e.g., does the functional failure constitute a hazard?).

4.1.5.3 Output of the FHA

Once an FHA is complete, the FHA report will identify functional hazards and safety critical functions.

4.1.5.4 Use of the FHA

The FHA is intended to be used as input into the OSA and subsequent safety analyses.

4.2 Other OSA Inputs

Other possible inputs for the OSA, especially if an FHA has not been conducted, are described in Section 4.2.1 through Section 4.2.7.

4.2.1 Solution ConOps

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

4.2.2 ANG-/SCT-Mandated Safety Analysis or Assessment Reports

These reports provide higher-level information possibly relevant to the OSA. This information may include proposed safety requirements and candidate hazards specifically targeted to the increment that the OSA is addressing.

4.2.3 OSED

Although the OSED is described within this guidance as an element of the overall OSA, an OSED may have already been developed as part of a Solution ConOps or an SCT-mandated analysis or assessment. If so, the OSED may be used as input or be further developed for the OSA in question.

4.2.4 FA

An FA examines a solution's functions and sub-functions that accomplish the operation or mission. An FA describes what the solution does, rather than how it does it, and is conducted at a level needed to support later synthesis efforts. Products from the FA such as the Functional Flow Block Diagram (FFBD) and N^2 diagram[5] may be used as inputs in developing the OSA. Other techniques may also be used to diagram solution functions.

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

4.2.5 Other OSAs

The legacy NAS is a "system of systems" that provides 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 also may build on one another, subsume each other, or combine for a joint function or capability. Thus, there must be a consistency of safety assessments across hierarchical levels from the program or system level up to the NAS level. Interactions and interdependencies across organizations, operational capabilities, NextGen portfolios, operational improvements, increments, and individual programs or solutions must be addressed in the OSA. Thus, OSAs developed for other solutions/capabilities may be important inputs to an OSA.

4.2.6 Shortfall Analysis

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

5. See the FAA SEM for further description of these processes.

4.2.7 Other Documentation

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

5 OSA Development Process

5.1 OSED Development Process

The OSED captures elements that comprise a CNS/ATM system (e.g., aircraft equipage, air traffic service provider technical systems, communication service provider systems, and procedural requirements), and it includes the operational performance expectations, functions, and selected technologies of the CNS/ATM system. The OSED facilitates the formulation of technical and procedural requirements based on operational expectations and needs.

Figure C.2 gives a logical overview of the steps required to conduct an OSED. Some of the steps may overlap or be iterative in nature.

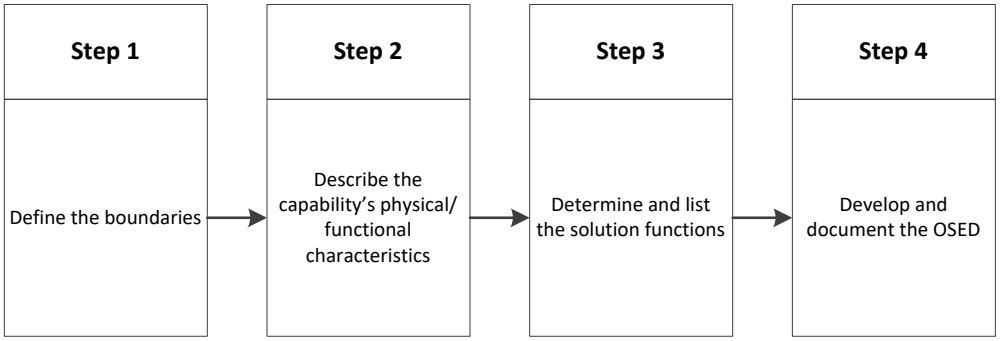

Figure C.2: OSED High-Level Process

The required tasks for preparing an OSED are described in Section 5.1.1 through Section 5.1.4.

5.1.1 Define the Boundaries

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

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

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

- The concept's state by including physical and functional characteristics,
- The environment's physical and functional characteristics,
- Air traffic services to be provided,

- Affected human elements (e.g., pilots, controllers, maintenance personnel, supervisors, etc.), and
- Operational procedures related to or affected by the concept.

5.1.3 Determine and List Functions

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

5.1.4 Develop and Document the OSED

Develop and document the OSED from the information obtained in the first three steps (i.e., the steps outlined in Section 5.1.1 through Section 5.1.3).

5.2 OHA Development Process

Once the solution has been bounded and described and the functions have been identified in the OSED, an SRM panel must identify the associated hazards via an OHA.[6] In developing an OHA, the panel must develop a PHL[7] using a systematic analysis of solution functions and functional failures to identify hazards. Each hazard must be subsequently classified according to its potential severity after considering causes and effects. The OHA uses the severity identified for each hazard to identify safety objectives and safety requirements for the solution that will result in an acceptable level of safety risk.

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

The OHA may be performed using either qualitative or quantitative methods. However, it is preferable to use quantitative data to support the assessment.[8] Figure C.3 provides an overview of the steps required to conduct an OHA.

6. The SMS Manual provides guidance on how to assemble SRM panels and facilitate the panel process.
7. The concept of the PHL is explained in the SMS Manual.
8. Various databases have been developed to support the SMS. Some of these are listed in the SMS Manual.

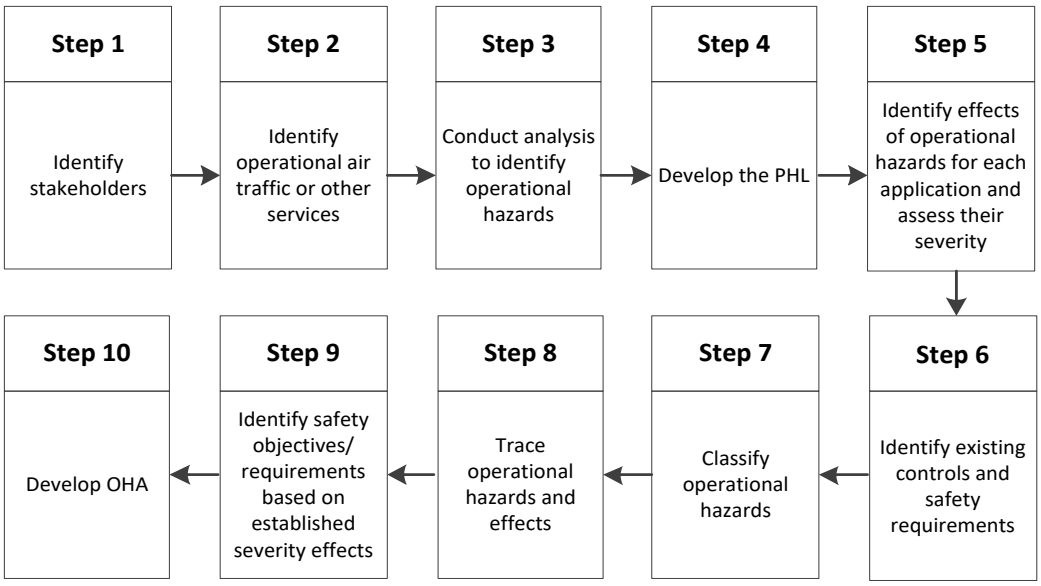

Figure C.3: OHA High-Level Process

The tasks required for preparing an OHA[9] are described in Section 5.2.1 through Section 5.2.9.

5.2.1 Identify Stakeholders

Identify applicants, approval authorities, and stakeholders needed to establish and demonstrate compliance with requirements for the air traffic service provision, its use, and any related CNS/ATM system. The stakeholders should also be SRM panel members, as practicable.

5.2.2 Identify Operational Air Traffic or Other Services

Copy the services provided by the solution that were documented in the OSED into the OHA.

5.2.3 Conduct Analysis to Identify the Operational Hazards

Identify the operational hazards. Document the analyses undertaken, linking the proposed improvement and the operational safety of the NAS elements—specifically the detailed, logical, and analytical connections. For these types of analyses, the most effective method is to “fail” each of the identified functions and their outputs. This is best done by “failing” the functions from the developed N^2 diagram or the FFBD, if available.

5.2.4 Develop the PHL

Review the hazards identified and develop a PHL that is concise, clear, and understandable; this PHL serves as the repository of the initial efforts of the SRM panel to identify all possible hazards. The PHL is refined and matured over time as the SRM panel validates the identified

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

hazards as credible and the OHA is further developed. The Bow-Tie Model[10] may be used as a tool for distinguishing between hazards, causes, and effects within the PHL.

5.2.5 Identify Controls and Safety Requirements

Identify the controls; the rationale for their use; and any supporting data that confirm the controls' use, applicability, and feasibility related to the hazard under consideration. Controls are measures, design features, warnings, and procedures that already mitigate credible outcomes (i.e., they have already been validated and verified as being effective). They may include procedural requirements as well as aircraft or ground system requirements related to the solution under review. The Bow-Tie Model (specifically the event tree side) can be used for identifying controls and safety requirements.

5.2.6 Identify Operational Hazard Effects

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

5.2.7 Classify Operational Hazards

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

The severity of each hazard is determined by the worst credible outcome or effect of the hazard on the solution or the NAS. The severity must be determined using a Bow-Tie Model or any other analysis tool, as appropriate.

5.2.8 Identify Safety Objectives

Establish overall safety objectives (either qualitative or quantitative) based on the operational hazard classifications. Assign a DAL to each function based on its severity. (As the design matures, the DALs may be reduced using architecture.) Once the safety objective is determined for each hazard, safety requirements can be written to ensure that the appropriate hazard controls are established as product requirements. Note that a requirement is a description of what must be done to achieve a safety objective.

5.2.9 Develop an OHA Worksheet

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

10. The Bow-Tie Model is a diagram of the hazard, the undesirable event, the trigger events or threats, potential outcomes, and the controls that minimize the risk. The methodology is an excellent way of visualizing risk management and communicating the context of the controls (barriers and mitigations) that manage or could manage risk.

Table C.1: OHA Worksheet Categories

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

Controls:

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

Severity and Safety Objectives:

Effect	Severity	Severity Rationale	Safety Objectives
The real or credible harmful outcome that has occurred or can be expected if the hazard occurs in the defined system state	The consequences or impact of a hazard's effect or outcome in terms of degree of loss or harm	Explanation of how severity was determined	Description of the safety objective to potentially mitigate the risk of the identified hazard to an acceptable level

5.3 ASOR Development Process

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

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

Figure C.4 provides an overview of the steps required to compile an ASOR.

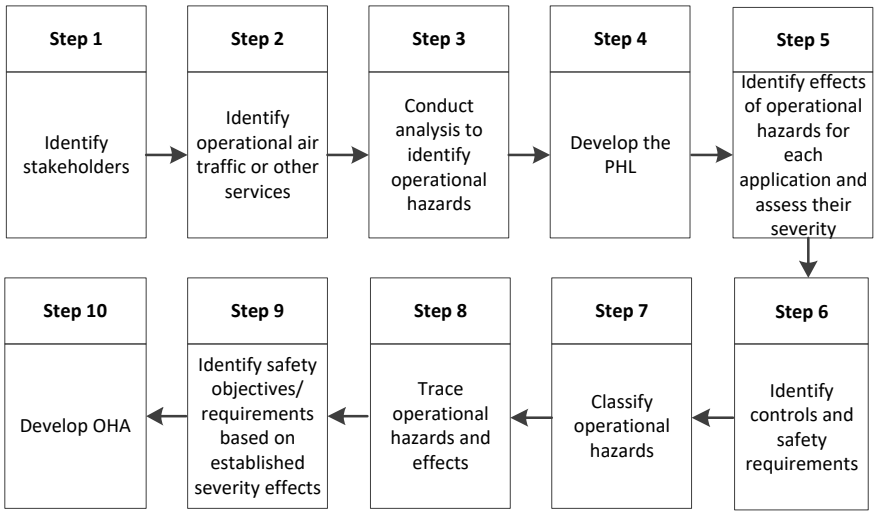

Figure C.4: ASOR High-Level Process

The tasks required for preparing an ASOR are described in Section 5.3.1 through Section 5.3.6.

5.3.1 Identify Solution Failure Relationships

Identify the relationships between CNS/ATM solution failures, procedural errors, and their effects on air traffic services and the hazard. Include identification of common cause failures and errors occurring among elements of the solution.

5.3.2 Identify Shared Risk Mitigation Strategies

Identify risk mitigation strategies that are shared by multiple elements of the CNS/ATM solution, including mitigation of effects from common cause failures and errors occurring across solution elements. CNS/ATM solution mitigation includes architectural and procedural aspects of the solution, as well as environmental mitigation and related candidate safety requirements identified in the OHA.

5.3.3 Develop and Reaffirm Safety Requirements

Reaffirm that the safety requirements developed from the shared risk mitigation strategies satisfy the safety objectives. The safety requirements identified must be complete, concise, clear, and necessary at the product level.

5.3.4 Allocate Safety Objectives and Requirements

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

5.3.5 Trace the ASOR Results to the OHA

Trace the ASOR results to each safety objective identified in the OHA.

5.3.6 Share Safety Objectives and Coordinate Safety Requirements

Coordinate the ASOR results such that:

- The impact of the ASOR on the NAS and other operational assessments is identified and reported.
- The impact of the ASOR on development and qualification of solution elements is identified and reported to the appropriate organizations. This impact includes criteria for quantifying safety objectives, identifying development assurance requirements, considering system architecture (including design features), and reducing the effects of generic design and implementation errors. Criteria for validating the effectiveness of procedural requirements must also be provided.

5.4 Assemble the OSED, OHA, and ASOR as an OSA and Prepare it for Approval

OSAs must be approved per the guidance in the SMS Manual. (*Note*: The PO must submit OSAs that support NAS acquisitions to the ATO Chief Safety Engineer for approval.[11]) The PO also must upload OSAs to SMTS per the instructions in the SMTS User Manual.

5.5 Validate OSA Results

Ensure the correctness and completeness of the safety objectives and requirements, including candidate safety requirements identified during the OHA. This ensures that requirements are necessary and sufficient for operational implementation. The validation may include analysis, simulation evaluations, concept testing, and operational trials. The validation includes a consistency check between the safety requirements and the OSED.

11. ANG is the review and acceptance authority for all OSAs prepared for the CRD phase of the AMS lifecycle. However, an OSA is not required for entrance into this phase.

Appendix D

Guidance for Conducting and Documenting a Comparative Safety Assessment

Guidance for Conducting and Documenting a Comparative Safety Assessment

1 Purpose

This guidance gives a process consistent with the Air Traffic Organization (ATO) Safety Management System (SMS) for conducting and documenting a Comparative Safety Assessment (CSA).

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the ATO SMS Manual, which provides guidance on fulfilling requirements set forth in the current version of FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements the FAA Acquisition Management System (AMS). Additionally, the systems engineering processes referred to are described in the FAA Systems Engineering Manual (SEM).

The primary reference materials in this guidance are the current editions of the following:

- AMS, Section 4.12, *National Airspace System Safety Management System*;
- SMS Manual;
- FAA Order JO 1000.37;
- FAA SEM; and
- Safety Management Tracking System (SMTS) User Manual.

3 Background

3.1 Description

A CSA provides management with a level comparison of all the identified potential safety hazards associated with meeting competing sets of operational requirements for alternate solution approaches and architectures. The CSA provides a more detailed safety risk assessment for each proposed investment alternative that is being considered, and it builds upon the assessments of likelihood of events identified in the previously conducted Operational Safety Assessment (OSA). Some alternatives that were not viable may have been discarded prior to this point. The remaining alternatives must now be complete, diverse, and technically viable.

The alternatives assessed may range from the reference case[1] of maintaining the status quo for implementing new designs, procedures, or program operational changes. The CSA determines the acceptability of each alternative from a safety risk perspective to allow informed and data-driven decisions to be made by FAA management. Other considerations in making a final alternative decision include cost, schedule, outside interdependencies, and training; however, they are not within the scope of a CSA. Those considerations are discussed in the Final Investment Analysis Plan or in Business Case Reports. CSAs are typically conducted internally by the Program Office (PO) with assistance from the Program Safety Team (PST).[2]

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

2. A PST is a resource provided by the PO to support the safety efforts of an acquisition throughout the AMS lifecycle. The PST is supported by a Safety and Technical Training safety case lead.

The Initial Investment Decision (IID) is the point at which the Joint Resources Council (JRC) approves or selects the best alternative that both meets the required performance and offers the greatest value to the FAA and its stakeholders. To support the IID, the PO must complete a CSA and, through Safety and Technical Training,[3] inform the JRC of the safety risk acceptability of each alternative.

A CSA is related to but different from an OSA. Where an OSA defines the target level of safety irrespective of the solution, a CSA provides an estimation of the potential safety risk associated with each proposed solution alternative.

3.2 Overview

The CSA is a risk assessment that defines severity and likelihood of the initial and predicted residual risk of each proposed alternative. The CSA builds upon an OSA (if one was previously conducted) by using the top-level Functional Analysis (FA) that was developed before the OSA. The FA is decomposed at least one more level in order to further expand the Preliminary Hazard List (PHL)[4] produced in the OSA. If an FA has not been previously developed, the PO must develop one as input to the CSA. If an OSA has not been previously conducted, then the PO must develop a PHL in the CSA. Figure D.1 provides an overview of the CSA development process.

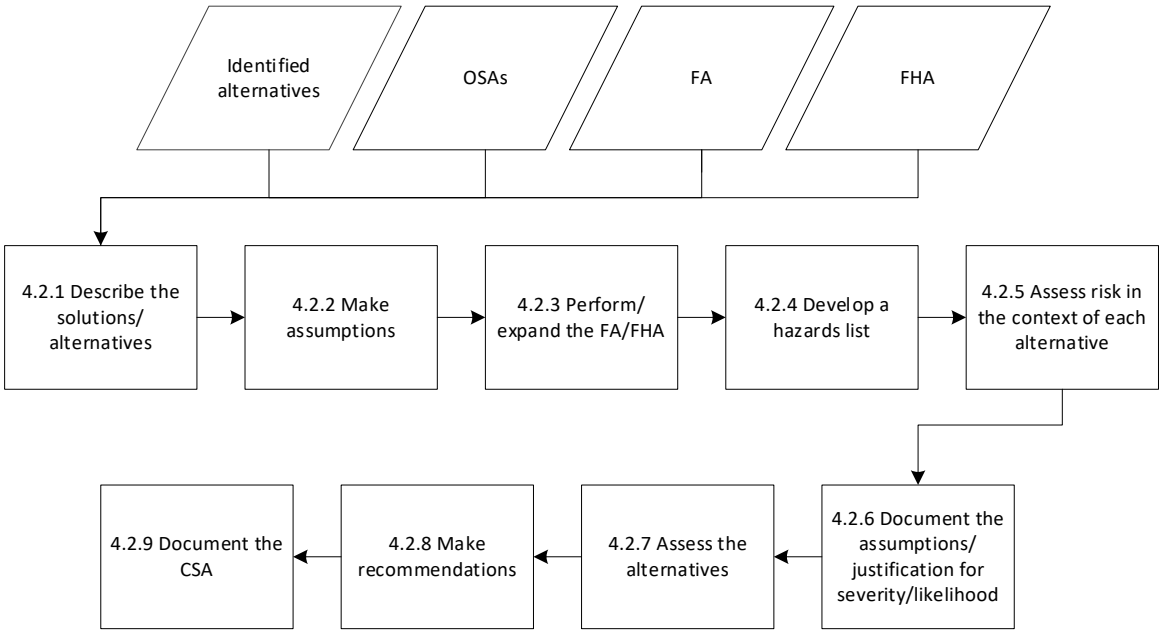

Figure D.1: The CSA Development Process

3.3 Use of Results

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

3.3.1 Preparing/Revising the Program Requirements Document

Controls from the reference case and generic safety requirements that are identified through the CSA process for each selected alternative (as yet solution agnostic) must be included in the Program Requirements Document. Related changes by alternative analyses must be

3. The ATO Chief Safety Engineer is responsible for this.
4. The concept of the PHL is explained in the SMS Manual.

separately documented. These changes include preliminary requirements from interdependent investments, new/modified air traffic control procedures, compliance with updates to the Code of Federal Regulations, and lifecycle-integrated logistics support (e.g., maintenance, training). At this stage, the initial Program Requirements Document (iPRD) defines the program's needs and requirements at a high level.

3.3.2 Establishing the Development Assurance Level

The Development Assurance Level (DAL) for each alternative (if applicable) is validated in the CSA. (*Note*: The DAL may differ among the investment alternatives assessed.)[5]

3.3.3 Preparing Safety Risk Management Documents

The output of the CSA should be used as an input to other Safety Risk Management (SRM) documents, particularly a Preliminary Hazard Analysis (PHA),[6] as the capability/solution alternative pros and cons are debated after the IID.

3.3.4 Preparing/Revising the Safety Requirements Verification Table

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

4 Procedures

This section describes the CSA development process.

4.1 Initial Inputs

The following are examples of inputs to the CSA.

4.1.1 Identified Alternatives

Investment analyses should bring at least three diverse, yet technically viable alternatives forward for selection of a preferred solution alternative. Ideally, the reference case is not one of these alternatives. Instead, it is a baseline against which the alternatives are compared. Consider the fact that the reference case is not always a "do-nothing" scenario, since many legacy program activities may already be in place and may go through some default evolution during the required implementation time of the alternative solutions. Therefore, potential safety consequences stemming from letting an existing system continue without further investment and without the targeted new capability must be fleshed out. This should address whether the targeted new capability is an improvement or a deterioration to the existing system.

4.1.2 OSAs

OSAs previously conducted for the Investment Analysis Readiness Decision may provide relevant information concerning safety hazards, causes, solution states, effects, and severity assessments to the CSA. Using these as inputs to the CSA, the likelihood of each hazard/cause/effect must be determined and matched with severity ratings. Differences among alternatives should begin to emerge, which could impact the combinations of cause/effect severity and likelihood ratings associated with each hazard. Ratings that are identical across all

5. The DAL for the eventually selected alternative is included in the iPRD and the initial Implementation Strategy and Planning Document prior to the Final Investment Decision (FID).

6. A PHA is best compiled after the alternatives are evaluated and a single alternative is selected as the best option. The PHA is conducted after the CSA and before the FID.

alternatives are eliminated as discriminators, leaving those that differ to be of prime importance to the CSA.

4.1.3 FA

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

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

4.1.4 Functional Hazard Assessment

A Functional Hazard Assessment (FHA) is a methodical approach to identifying credible operational safety effects through the assessment of system or sub-system functions and failure conditions. The FHA identifies and classifies the system functions and safety hazards associated with functional failure or malfunctions. It identifies the relationships between functions and hazards, thereby identifying the safety-significant functions of the system as well as the hazards associated with that functionality. This identification provides a foundation for the safety program to scope additional safety analyses.

4.2 CSA Development Process

4.2.1 Describe the Solutions/Alternatives

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

4.2.2 Make Assumptions Only If Specific Information Is Not Available

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

4.2.3 Perform/Expand the FA/FHA

Perform an FA/FHA (or expand the one previously developed) in accordance with the FAA SEM and Safety Risk Management Guidance for System Acquisitions Appendix C. Attempt to match similar and unique causes associated with each hazard into a firm list of unique events that may be adequately addressed by existing functions or by postulating new low-level system functions. This analysis results in complete sets of hierarchical functions that alternative system solutions must perform.

Look for matches between system function and mitigation of all causes (within system bounds). Organize causes that fall beyond system bounds into assumptions and constraints for

coordination with external NAS entities. Though all such external dependencies may be noted, it may not be possible to address them within the bounds of this system.

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

Decide which alternative solutions remain viable after a cursory look at safety. Discard any potential solution "fragments"[7] that inadequately address safety concerns.

4.2.4 Develop a Hazards List

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

Table D.1: CSA Hazards List

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

4.2.5 Assess Risk in the Context of Each Alternative

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

4.2.6 Document the Assumptions and Justifications

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

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

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

4.2.7 Assess Each Alternative from a Safety Perspective

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

Table D.2: CSA Worksheet Categories

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

Controls:

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

Initial Risk:

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

4.2.8 Assess Development Assurance Risk

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

4.2.9 Establish Safety Requirements and Predict Residual Risks

For each alternative, establish:

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

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

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

Table D.3: Safety Requirements and Residual Risks

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

4.2.10 Make Recommendations Based on the Data in the CSA

For decision-making purposes, compare the results of the safety risk assessment of each alternative considered. Compile the results in Table D.4. (*Note*: Not all hazards may apply to each alternative assessed. Enter "N/A" in Table D.4 when appropriate.) Ensure the decision

makers can clearly distinguish the safety merit of each alternative. Prepare an executive summary that clearly states whether the CSA finds all alternatives alike or whether one or two particular alternatives are clearly superior to others on the basis of safety risk.

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

Table D.4: Comparison of Safety Assessments

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

4.2.11 Document, Assemble, and Prepare the CSA for Approval

CSAs must be approved per SMS Manual guidance. The CSAs must be uploaded to SMTS following the instructions in the SMTS User Manual.

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

4.3 Validate the CSA Results

For typical programs, safety requirement validation for the down-selected alternative is conducted following the Final Investment Decision. Validation ensures the correctness and completeness of the safety objectives and requirements, including candidate safety requirements. This ensures that the safety requirements are necessary and sufficient for operational implementation.

Appendix E

Guidance for Conducting and Documenting a Preliminary Hazard Analysis

Guidance for Conducting and Documenting a Preliminary Hazard Analysis

1 Purpose

This guidance gives a process consistent with the Air Traffic Organization (ATO) Safety Management System (SMS) for conducting and documenting a Preliminary Hazard Analysis (PHA) of the program approved at the Final Investment Decision (FID).

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the ATO SMS Manual, which provides guidance on fulfilling requirements set forth in the current version of FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements the FAA Acquisition Management System (AMS). Additionally, the systems engineering processes referred to are described in the FAA Systems Engineering Manual (SEM).

The primary reference materials in this guidance are the current editions of the following:

- AMS, Section 4.12, *National Airspace System Safety Management System*
- SMS Manual
- FAA Order JO 1000.37
- FAA SEM
- Safety Management Tracking System (SMTS) User Manual

3 Background

3.1 Description

For system acquisitions, the PHA[1] is a broad initial hazard identification process conducted by the Program Office (PO) during the Investment Analysis phase of an acquisition. It is a systematic and detailed hazard analysis of system hardware and software, the environment in which the system exists, and the system's intended use or application. It focuses on the details of the early system design (including possible implications) and is primarily used to perform a safety risk assessment to develop early safety-related requirements and specifications and to support the Verification and Validation (V&V) of existing safety requirements. The PHA technique focuses on identifying potential hazards early in the life of a system, thus saving time and money that might be required for major redesign if those hazards were discovered at a later date.

The PHA follows the DIATT (**D**escribe the system, **I**dentify hazards, **A**nalyze risk, **A**ssess risk, **T**reat risk) process identified in the SMS Manual by identifying potential safety hazards, ranking them according to their severity and likelihood, and translating these potential hazards into high-level system safety design constraints and hazard controls (See Figure E.1).

The output of the PHA is used to develop system safety requirements and to assist with preparing performance and design specifications. In addition, the PHA is often a precursor to more detailed safety risk assessments (e.g., System Hazard Analysis or Sub-System Hazard Analysis), as additional safety analyses are generally required to more fully understand and

1. A PHA is not the same as a Hazard Analysis Worksheet, which is used to tabulate the PHA findings.

evaluate safety hazards identified by the Safety Risk Management (SRM) panel. Per the AMS, completion of the PHA is also a requirement for consideration at the FID.

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

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

The PHA is often conducted in-house by the PO. However, if contracted out, a suggested Data Item Description (DID) may be found in the DID Library. The PO may tailor the DID as necessary.

3.2 Use of Results

The PHA results may be used to:

- Identify safety requirements to include in the final Program Requirements Document.
- Highlight significant safety risks.
- Identify safety risk issues.
- Identify improvement opportunities and make recommendations concerning the elements of the system that are most likely to contribute to future problems.
- Develop specific suggestions for improving future activity or system performance, including:
    - Equipment modifications,
    - Procedural changes, or
    - Administrative policy changes.
- Develop system safety requirements by:
    - Preparing design descriptions.
    - Recommending additional safety risk assessments. As suggested by the name, the PHA is conducted in an early phase of a project. The insights gained from the PHA help determine which, if any, additional safety risk assessments should be conducted and serve as input to more detailed safety risk analyses. The recommendations for additional analyses must be reflected in the PSP.
- Serve as input into subsequent safety analyses.

3.3 Hazard Analysis Techniques

The SMS Manual and the FAA SEM describe various hazard analysis techniques that may be used in developing the Hazard Analysis Worksheet (HAW) of the PHA.

These techniques include:

- Function failure analysis,
- Event tree analysis,
- Failure modes and effects analysis,
- Fault tree analysis,
- Cause-consequence diagram, and
- “What if” analysis.

4 Procedures

4.1 Overview

Figure E.1 shows the PHA high-level process.

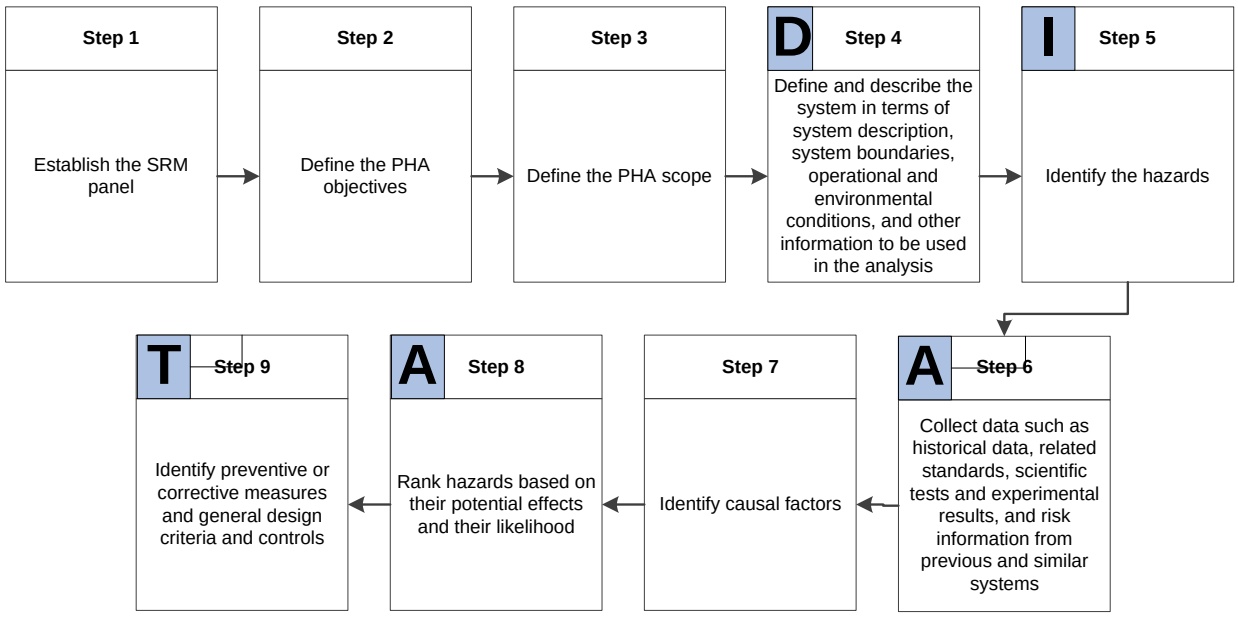

Figure E.1: PHA High-Level Process

4.2 Inputs

The following list describes possible inputs to the PHA.

- **System Description:** A description of the system under development and the context in which it is to be used, including layout drawings, process flow diagrams, and block diagrams.
- **Safety Data:** Historical hazard data (including lessons learned from other systems) that allow the incorporation of experience gained from previous operation of the same system or similar systems. Potential data sources are listed in the SMS Manual.
- **Functional Analysis (FA):** An expansion of the FAs conducted to support the Operational Safety Assessment (OSA) or Comparative Safety Assessment (CSA) conducted earlier in the AMS lifecycle.

- **Functional Hazard Assessment**: A methodical approach to identifying credible operational safety effects through the assessment of system or sub-system functions and failure conditions.
- **Preliminary Hazard List:** A list of hazards determined in previous safety analyses or brainstorming.
- **Hazard Checklist:** A list of the causes of safety incidents with the same or similar equipment.
- **Customer Requirements:** Any pre-existing requirement specifications and concept documents.
- **Regulatory Requirements:** Constraints imposed by regulatory agencies.
- **Previously Conducted Safety Analyses:** Any relevant information from safety assessments (e.g., OSAs, CSAs, or Safety Collaboration Team studies) already conducted.
- **Development Assurance Levels (DALs):** The DAL is the mitigation for a hazard of a design error. Each function should consider the result of a design error causing a loss of function or misleading function and assign an appropriate system, hardware, and software DAL.

4.3 Content

The PHA must be written in accordance with the requirements of the SMS Manual. Table E.1 is the basic HAW that is used to develop the PHA. The description of each identified hazard must contain, at a minimum, the information presented in Table E.1.

Table E.1: Components of a HAW

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

Controls:

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

Initial Risk:

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

Safety Requirements:

Safety Requirement Description	Planned for Implementation?	Organization Responsible for Implementing Safety Requirement	Point of Contact (POC)
A planned or proposed means to reduce a hazard's causes or effects	Denotes whether the safety requirement is planned for implementation (Yes/No)	The organization's name / routing code	POC's name and telephone number

Predicted Residual Risk:

Predicted Residual Risk	Predicted Residual Risk Rationale
The risk that is estimated to exist after the safety requirements are implemented or after all avenues of risk mitigation have been explored	If necessary, any additional explanation needed to help the reader understand how the predicted residual risk was determined

Safety Performance Target:

Safety Performance Target
The measurable goals that will be used to verify the predicted residual risk of a hazard

4.4 PHA Documentation and Preparation for Approval

The information in Table E.1 must be used as an input for SMTS, which generates the PHA documentation. Instructions for entering information into SMTS are in the SMTS User Manual. PHAs must be reviewed in accordance with the Safety and Technical Training–facilitated peer review process and approved per the guidance given in the Safety Risk Management Guidance for System Acquisitions and the SMS Manual.

The PO must enter into SMTS safety hazards and requirements identified in the PHA so that subsequent V&V activities may be tracked and monitored.

4.5 PHA Updates

If any subsequent analysis identifies a safety hazard that cannot be traced back to one identified in the PHA, the PO must update the PHA and submit it for approval by the ATO Chief Safety Engineer.

Uncontrolled copy when downloaded

Appendix F

Guidance for Conducting and Documenting a Sub-System Hazard Analysis

Guidance for Conducting and Documenting a Sub-System Hazard Analysis

1 Purpose

This guidance describes the Sub-System Hazard Analysis (SSHA), which is an update to a Safety Risk Management (SRM) document that is consistent with the Air Traffic Organization (ATO) Safety Management System (SMS).

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the ATO SMS Manual, which provides guidance on fulfilling requirements set forth in the current version of FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements the FAA Acquisition Management System (AMS). Additionally, the systems engineering processes referred to are described in the FAA Systems Engineering Manual (SEM).

The primary reference materials in this guidance are the current editions of the following:

- AMS, Section 4.12, *National Airspace System Safety Management System*;
- SMS Manual;
- FAA Order JO 1000.37;
- FAA SEM; and
- Safety Management Tracking System (SMTS) User Manual.

3 Background

3.1 Overview

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

The SSHA takes the previously identified hazards that originated in the Preliminary Hazard Analysis (PHA) and any other sources; considers the sub-system design and architecture; and refines those hazards through analytical selection, decomposition, and traceability. Sometimes this analysis uncovers new hazards that manifest because of an implementation choice.

The analysis focuses on failure modes as they contribute to hazards at the sub-system level and investigates the detailed interfaces between components for possible conditions leading to hazards. In addition, the analysis focuses on component and equipment failures or faults and human errors that establish a hazard due to the functioning of the sub-system.

Sub-systems may be a single media type (e.g., electronic, software, or mechanical). In addition, there may be mixed-media sub-systems such as embedded software-hardware systems or

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

electromechanical actuators that require a more integrated SSHA. In either case, the human is considered a component that both receives inputs and initiates outputs within a sub-system.

The SSHA is conducted at a greater level of detail than a PHA and is intended to show that the sub-system design meets safety requirements. The analysis is completed by reviewing design drawings, engineering schematics, and specifications. As the system and related sub-systems are further defined and system design changes (including software design changes) are implemented, the system developer must revise the SSHA as necessary.

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

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

Due to the complexity of the SSHA, the analysis is usually identified in a procurement specification and conducted by the system developer. If so, the PO must include the need to conduct an SSHA as a contractual requirement. The PO must also require that SRM panels be conducted. Further, if facilitated or conducted by the developer, the panels must include Subject Matter Experts, particularly those with an operational perspective. The FAA must actively review and be able to modify/comment on the safety analysis documentation as it is being prepared by the developer and not just at its final delivery. The developer must incorporate any valid comments received from the government's peer review process. A suggested Data Item Description (DID) can be found in the DID Library. The PO may tailor the DID as necessary.

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

3.2 Use of the Analysis

An SSHA must:

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

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

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

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

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

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

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

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

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

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

3.3 Software Aspects of Analysis

Software guidance may be reviewed in the following sections of the Safety Risk Management Guidance for System Acquisitions:

- Section 2.3.2.1.4, System Development Assurance (for the Investment Analysis Readiness Decision);
- Section 2.3.3.1.2.1, System Development Assurance (for the Initial Investment Decision);
- Section 2.3.4.1.2.1, System Development Assurance (for the Final Investment Decision);
- Section 2.3.5.1.3, System Development Assurance (for the ISD);
- Section 6.3, Managing Software Risk;
- Section 9.4, Software-Intensive Systems;
- Appendix A, Guidance for Preparing and Implementing Program Safety Plans, Section 5.1.3, Identify Developmental Assurance Requirements; and
- Appendix M, Overview of RTCA DO-278A and Its Required Deliverables.

The Development Assurance Level (DAL) is based on hazards identified during the SRM process. Until this point, the SRM process was conducted without any specific details about

implementation and thus had to rely on assumptions about how the system would behave. As part of the sub-system, the software is addressed in the SSHA by the system developer. Individuals performing an analysis on the system may not necessarily be experts in software behavior. In addition, the software developer may be a subcontractor to the system developer. Thus, it is critical that the SSHA process address how the software analysts and system analysts communicate and understand each other. The software aspects of hazard analysis must ensure (1) the people doing the safety analysis know enough about the software implementation details to ensure the safety analysis is still valid and (2) these people are not surprised by an unexpected implementation method. Although the term “software hazard analysis” is sometimes used, the SSHA process is concerned with the software portion of the system analysis. The SSHA is used to validate the assumptions made in the PHA.

The choice of system design and architecture can invalidate current safety requirements and pose unanticipated hazards that could generate new safety requirements potentially affecting the DAL. For example, architectural mitigation and partitioning techniques may be used in order to reduce the DAL. If DAL reduction is proposed, then the PO must be informed to ensure the reduction can be evaluated and approved.

The SSHA process is iterative, beginning as a preliminary analysis early in the design development. It matures to eventually document the state of the final system. Early in development planning, the SSHA can:

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

As the design progresses, the SSHA will:

- Ensure that the method for software design, requirements specification, implementation, and corrective action planning does not impair or decrease the safety risk associated with the sub-system; and evaluate any new safety hazards introduced into the system;
- Design and analyze the human-computer interface;
- Develop safety-related information for operations, maintenance, and training manuals; and
- Evaluate whether potential changes to the software could affect safety.

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

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

The SSHA documents how the software performs its intended function safely. It does this by:

- Ensuring that the safety design criteria identified in the software requirement specifications have been satisfied and
- Ensuring that the implementation choices have been evaluated so no unsafe conditions have been introduced.

3.4 Other Considerations

- The PO must refer to the program-specific Program Safety Plan (PSP) approved by the ATO Chief Safety Engineer to determine which safety assessments must be conducted during a system acquisition.
    - The PO may use methods other than SSHA to capture required information or may prepare a combined SSHA / System Hazard Analysis (SHA) to meet AMS requirements only if such alternatives have been approved in the PSP.
- The system safety process is a set of analyses that starts at the PHA and continues through the SSHA, SHA, and Operating and Support Hazard Analysis. Each analysis gets more discrete as more design details are known.
    - The basis of each analysis is a Hazard Analysis Worksheet (HAW). The HAW, initially developed early in the system lifecycle (i.e., during the PHA), is further developed, modified, and enhanced as subsequent analyses are conducted.
    - Each subsequent analysis has a slightly different focus but is essentially a HAW that builds on a previously developed HAW.
    - An SSHA is considered to be an update to the previous SRM document prepared for the acquisition system.
- SSHAs are developed for new systems; however, many acquisition programs deploy their capabilities incrementally over time and have an Initial Operating Capability date for each capability. In lieu of a new SSHA, additions to previously developed systems may require either updates to existing SSHAs, supplemental hazard analyses, or new hazard analyses. The specifics of such analyses must be defined in the approved PSP.
- Using a Commercial Off-the-Shelf (COTS) product with a very high reliability as a sub-system or component of a sub-system will not automatically ensure a safe system, as reliability does not account for interactions with other system components. This is particularly important to remember with software because it usually controls many, if not all, of the interactions among system components. Simply equating software reliability or specification conformance with safety will not ensure an acceptable safety level of the system. There may be times when it is less expensive and safer to provide special-purpose software rather than a COTS product; using COTS may amount to a false economy.
- There are other times where COTS components may have adequate system safety. In these cases, the producer of that component must provide the prime contractor with either a complete “black box” behavior specification or an analysis that shows the component design allows protection against any possible hazardous software behavior. This information must be provided for a complete SSHA to be performed.

- If the SSHA identifies a safety hazard that is new or cannot be traced back to a hazard identified in the PHA, the PO must update the PHA and submit it for approval by the ATO Chief Safety Engineer.
- DALs from previous analyses should be revisited with the available design information.

4 Preparing the SSHA

4.1 Initial Inputs

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

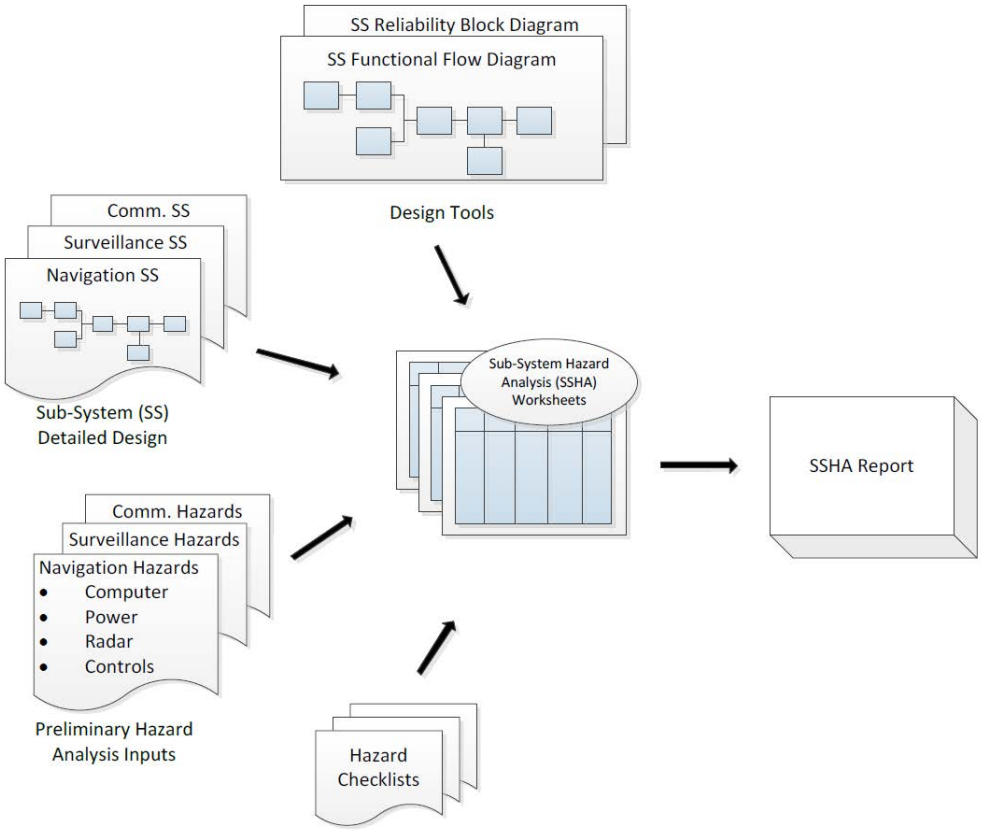

Figure F.1: Inputs to the SSHA

4.2 Hazard Analysis Techniques

Refer to the SMS Manual and the FAA SEM for descriptions of various hazard analysis techniques that may be used in developing an SSHA. These techniques include:

- Function failure analysis,
- Event tree analysis,
- Failure modes and effects analysis,
- Fault tree analysis,[2]

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

- Cause-consequence diagram use, and
- “What if” analysis.

4.3 Conducting the SSHA

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

5 Reviewing and Approving the SSHA

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

6 Preparing and Revising the Safety Requirements Verification Table

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

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

Appendix G

Guidance for Conducting and Documenting a System Hazard Analysis

Guidance for Conducting and Documenting a System Hazard Analysis

1 Purpose

This guidance describes the System Hazard Analysis (SHA), which is an update to a Safety Risk Management (SRM) document that is consistent with the Air Traffic Organization (ATO) Safety Management System (SMS).

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the ATO SMS Manual, which provides guidance on fulfilling requirements set forth in the current version of FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements the FAA Acquisition Management System (AMS). Additionally, the systems engineering processes referred to are described in the FAA Systems Engineering Manual (SEM).

The primary reference materials in this guidance are the current editions of the following:

- AMS, Section 4.12, *National Airspace System Safety Management System*
- SMS Manual
- FAA Order JO 1000.37
- FAA SEM
- Safety Management Tracking System (SMTS) User Manual

3 Background

3.1 Overview

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

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

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

Safety design requirements (some of which were generated during the PHA) that are included in the final Program Requirements Document are refined during the SHA; the system must be validated for conformance to these requirements. Through the SHA, safety design

requirements are traced to individual components based on functional decomposition and allocation. As the system design matures, the SHA should be updated.

The Program Office (PO) must refer to the program-specific Program Safety Plan (PSP) approved by the ATO Chief Safety Engineer to determine which safety analyses/assessments must be conducted during a systems acquisition. The PO may use methods other than an SHA to capture required information or may prepare a combined SSHA/SHA to meet AMS requirements only if such alternatives have been approved in the PSP.

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

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

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

3.2 Use of the Analysis

An SHA assesses the risks associated with the total system design (including software) by recognizing previously unidentified hazards associated with system interfaces, system functional faults, and system operation in the specified environment. It determines whether the method of implementing the hardware, software, facility design requirements, and corrective actions has impaired or degraded the safety of the system or introduced any new hazards. An SHA must also consider human factors, system/functional failures, and functional relationships between the sub-systems comprising the system (including software). An SHA recommends new/modified system requirements to eliminate identified hazards or to control their associated risk to acceptable levels, refines high-level safety design requirements, and provides a comprehensive analysis baseline for subsequent design changes.

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

4 Analysis Tools

In an SHA, a hazard causal analysis[1] is used to refine the high-level safety requirements into more detailed requirements. This process typically requires a model of the system. Causal

1. In simple terms, a causal analysis is a process used to identify why something occurs. See the FAA SEM for further details.

Uncontrolled copy when downloaded

analysis usually involves a search through the system design for system states[2] or conditions that could lead to system hazards.

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

- Fault tree analysis,
- Failure modes and effects analysis,
- Event tree analysis, and
- Interface analysis.

5 Preparing the SHA

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

Inputs into the SHA include:

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

The SHA may be used to identify:

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

6 Traceability to the PHA

If the SHA identifies a safety hazard that is new or cannot be traced back to one identified in the PHA, then the PO must update the PHA and submit it for approval by the ATO Chief Safety Engineer.

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

Uncontrolled copy when downloaded

7 Reviewing and Approving the SHA

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

8 Preparing/Revising the Safety Requirements Verification Table

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

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

Appendix H

Guidance for Conducting and Documenting an Operating and Support Hazard Analysis

Guidance for Conducting and Documenting an Operating and Support Hazard Analysis

1 Purpose

This guidance describes the Operating and Support Hazard Analysis (O&SHA), which is an update to a Safety Risk Management (SRM) document that is consistent with the Air Traffic Organization (ATO) Safety Management System (SMS).

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the ATO SMS Manual, which provides guidance on fulfilling requirements set forth in the current version of FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements FAA Acquisition Management System (AMS) policy. Additionally, the systems engineering processes referred to are described in the FAA Systems Engineering Manual (SEM).

The primary reference materials in this guidance are the current editions of the following:

- AMS, Section 4.12, *National Airspace System Safety Management System*;
- SMS Manual;
- FAA Order JO 1000.37;
- FAA SEM; and
- Safety Management Tracking System (SMTS) User Manual.

3 Background

3.1 Overview

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

The purpose of the O&SHA is to identify and evaluate the safety risk of NAS operations derived from the implementation of operating and support tasks. These tasks encompass procedures conducted by air traffic controllers as well as support functions conducted by aviation safety specialists. The O&SHA ensures that any safety risk in NAS operations resulting from interactions of the personnel performing system operation/support functions remains at an acceptable level. This analysis technique, which uses methodology similar to that of the Preliminary Hazard Analysis (PHA), identifies safety hazards presented in operating and support tasks as they impact NAS operations, along with their safety hazard causal factors and effects. The O&SHA analyzes the safety risk of NAS operations by evaluating operating and support procedures, the system design, and the human-system integration interface. In addition, it proposes mitigations to the hazards identified from the analysis of these procedures and support functions.

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

Uncontrolled copy when downloaded

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

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

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

Due to the complexity of the O&SHA, the analysis is usually identified in a procurement specification and conducted by the system developer. If so, the change proponent (most likely the Program Office (PO)) must include the need to conduct an O&SHA as a contractual requirement. The PO must also require that an SRM panel be conducted and that all SRM panels facilitated or conducted by the developer include subject matter experts, particularly those with an operational perspective. The government must actively review and be able to modify/comment on the safety analysis documentation as it is being prepared by the developer and not just at its final delivery. The developer must incorporate any valid comments received from the government's peer review process. A suggested Data Item Description (DID) can be found in the DID Library. The PO may tailor the DID as necessary.

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

3.2 O&SHA Goals

The goals of the O&SHA are to:

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

3.3 O&SHA Scope

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

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

An O&SHA provides:

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

3.4 Inputs

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

- Previous safety analyses (e.g., PHAs, System Hazard Analyses or Sub-System Hazard Analyses).
- Procedures.
- Sequence diagrams.
- Operation and functional analyses.
- Equipment layout diagrams.
- System and sub-system design specifications.
- Equipment and interface drawings.
- Operations and maintenance instructions.
- Human factors engineering data.
- Task design.
- System/operational design.
- Hardware failure modes.

4 Preparing the O&SHA

4.1 Analyzing Procedures

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

- Required tasks, the human-machine environment, interpersonal interactions, and the sequence of operating/support steps will not create an unacceptable safety risk to NAS operations;
- Procedures do not expose personnel to any unacceptable safety hazards that may impact NAS operations;

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

4.2 Methodology

The methodology of conducting an O&SHA matches that of a PHA. To ensure procedures focus on NAS operational safety (as opposed to safety impacts to the operators/maintainers), the change proponent must:

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

5 Traceability to the PHA

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

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

6 Reviewing and Approving the O&SHA

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

7 Preparing/Revising the Safety Requirements Verification Table

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

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

Appendix I

Guidance for Documenting a System Safety Assessment Report

Guidance for Documenting a System Safety Assessment Report

1 Purpose

This guidance describes the System Safety Assessment Report (SSAR), which is the final pre-deployment update to a Safety Risk Management (SRM) document portfolio that is consistent with the Air Traffic Organization (ATO) Safety Management System (SMS).

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the ATO SMS Manual, which provides guidance on fulfilling requirements set forth in the current version of FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements FAA Acquisition Management System (AMS) policy. Additionally, the systems engineering processes referred to are described in the FAA Systems Engineering Manual (SEM).

The primary reference materials in this guidance are the current editions of the following:

- AMS, Section 4.12*, National Airspace System Safety Management System*
- SMS Manual
- FAA Order JO 1000.37
- NAS SEM
- Safety Management Tracking System (SMTS) User Manual

3 Background

3.1 Scope of the SSAR

The SSAR confirms that appropriate system safety engineering was performed during system development prior to deployment into the NAS by:

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

3.2 Overview

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

For systems undergoing Independent Operational Assessment (IOA), the SSAR must be updated to reflect IOA results, as appropriate. Safety findings documented during the IOA must

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

be evaluated by the Program Office (PO) to determine whether further analysis is needed; as necessary, appropriate mitigations and a monitoring plan must be developed for safety hazards identified in the IOA. For small development programs or non-developmental item acquisitions for products with low safety risk hazards, the SSAR may be the only formal documentation of safety program activities / hazard assessment.

The SSAR must be developed by the FAA change proponent, most likely representing the PO, as a summary document. However, due to the complexity of the SSAR, the change proponent usually identifies the development of the SSAR as a requirement that must be included in the development/acquisition contract and conducted by the system developer. The change proponent should include the need to prepare an SSAR as a contractual requirement in Section C of the contract. A suggested Data Item Description (DID) can be found in the DID Library. The PO may modify the DID as necessary.

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

- Submit the SSAR to Safety and Technical Training (AJI) for peer review and
- Ensure that the document is signed and approved per SMS Manual requirements.

4 SSAR Input

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

- Testing
  - Development testing
  - Operational testing
  - Acceptance testing
  - Field familiarization
- IOA
- Operational Suitability Demonstration[2]
- SRM documents
  - Operational Safety Assessment
  - Comparative Safety Assessment
  - Preliminary Hazard Analysis (PHA)
  - Sub-System Hazard Analysis

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

- System Hazard Analysis
- Operating and Support Hazard Analysis

- Development Assurance documentation (e.g., the Plan for Software Aspects of Approval, Software Accomplishment Summary, and evidence of compliance)
- Post-Implementation Review (PIR)
- Other analyses, assessments, and tests

5 SSAR Organization

The SSAR must contain the elements described in Section 5.1 through Section 5.11 of this appendix.

5.1 Signature Page

The signature page includes the appropriate signature blocks for safety risk acceptance and SRM document approval. (See Section 7 of this appendix.)

5.2 Executive Summary

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

5.3 System Description

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

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

5.4 System Operations

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

- The procedures for operating, testing, and maintaining the system, including a discussion of the safety design features and controls incorporated into the system as they relate to the operating procedures;

- Any special safety procedures needed to assure safe operation, testing, and maintenance, including emergency procedures;
- Anticipated operating environments and any specific skills required for safe operation, testing, maintenance, transportation, or disposal; and
- Any special facility requirements or personal equipment to support the system.

5.5 System Safety Engineering

This section must include a description of or reference to:

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

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

This section summarizes the results of the analyses performed and the tests conducted. It must contain a compliance assessment and sufficient evidence to demonstrate compliance with development assurance requirements (like those of RTCA[3] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*).

5.7 Hazards Identification

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

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

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

5.8 Safety Requirements Verification Table

The Safety Requirements Verification Table (SRVT) is an evolving list of safety requirements that starts with a system's first safety assessment. It lists the safety requirements that have been verified and the status of requirements not yet verified (including information on when they will be verified).[4] The PO must ensure all safety requirements are captured within the SRVT.

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

4. Safety requirements are controls written in requirements language; they are used to mitigate the risk associated with identified hazards.

The SRVT must contain the following information:

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

5.9 Monitoring Plan

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

However, this V&V of safety requirements does not eliminate the need for monitoring the safety performance of the fielded system. The PO must establish safety performance targets for all hazards that were identified in the PHA and develop an operational monitoring plan to track these performance targets. The duration of the monitoring activities will depend on the complexity of the system being deployed, the sites at which the system will be deployed, and the nature of the established performance targets. The risk acceptor or his or her designee must conduct the monitoring.

The PO must also recognize that:

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

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

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

5.10 Conclusions and Recommendations

This section must include:

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

5.11 References

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

6 Accomplishing the SSAR

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

- Periodic review: These reviews are conducted throughout the life of the program. They evaluate the status of the hazards based on the verification of controls and requirements and help in monitoring control effectiveness.
- Phased review: These reviews are conducted for defined portions of the implementation of solutions in the NAS. Phased reviews apply to a single Joint Resources Council decision, which involves implementing a solution in steps or phases. As long as the implementation is incremental (i.e., performed in steps), each increment involves safety reviews to evaluate the status of hazards based on the verification of mitigating requirements for that particular phase.
- Final implementation review: These reviews are conducted for a program's ISD or IOC declaration.

7 Technology Refreshment Portfolio

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

8 Approving the SSAR

The SSAR must be reviewed in accordance with the AJI-facilitated peer review process and approved per the guidance provided in the SMS Manual. The PO must upload the SSAR to SMTS per the instructions found in the SMTS User Manual. The ATO Chief Safety Engineer will not approve the SSAR if there is insufficient evidence of compliance with RTCA DO-278A.

Appendix J

Development Assurance for Communication, Navigation, Surveillance and Air Traffic Management Systems

Development Assurance for Communication, Navigation, Surveillance, and Air Traffic Management Systems

1 Purpose

This guidance provides development assurance methods for ground systems that affect the safety of operations in the National Airspace System (NAS).

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the Air Traffic Organization (ATO) Safety Management System (SMS) Manual, which provides guidance on fulfilling requirements set forth in the current version of FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements the FAA Acquisition Management System (AMS).

The primary reference materials in this guidance are the current editions of the following:

- AMS, Section 4.12, *National Airspace System Safety Management System*;
- SMS Manual;
- FAA Order JO 1000.37;
- FAA Order 8100.8, *Designee Management Handbook*;
- FAA Advisory Circular (AC) 20-171, *Alternatives to RTCA/DO-178B for Software in Airborne Systems and Equipment*;
- The current version of SAE Aerospace Recommended Practice (ARP)[1] ARP4754A, *Guidelines for Development of Civil Aircraft and Systems*; and
- The current version of each of the following RTCA[2] documents:[3]
    - RTCA DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*;
    - RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*;
    - RTCA DO-248C, *Supporting Information for DO-178C and DO-278A*;
    - RTCA DO-330, *Software Tool Qualification Considerations*;
    - RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A*;
    - RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*; and

1. An ARP is a guideline from SAE International.

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

3. An RTCA user identity and password are required to download RTCA documents. FAA employees may obtain an RTCA membership by contacting RTCA.

- RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*.
- RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*

3 Background

AMS, Section 4.12, requires that products be developed at a rigor commensurate with the severity of the associated hazard should that product experience a failure. This includes system, hardware, and software development. For software-intensive systems, the establishment of a development assurance program in accordance with RTCA DO-278A is an acceptable means. However, it is not the only method of demonstrating that a software product was developed at the appropriate level of rigor. Refer to Section 6.7 of this appendix for alternative methods.

RTCA DO-248C provides clarification of the guidance material in RTCA DO-178C and RTCA DO-278A and should be used as a companion document when seeking additional information for understanding. References to RTCA DO-178C are provided for comparison since these considerations concern airborne systems.

RTCA DO-330 is a standalone document that provides software tool qualification guidance. Refer to Section 6.5 of this appendix for information regarding how RTCA DO-330 relates to RTCA DO-278A.

When using RTCA DO-278A as the means of compliance with AMS policy, the associated RTCA DO-278A supplements must also be used where applicable. RTCA DO-331, RTCA DO-332, and RTCA DO-333 address certain software development techniques and can add, delete, or modify objectives, activities, and lifecycle data in RTCA DO-278A. Guidance within a particular supplement should be applied when using the addressed technique.

4 Why Development Assurance

The purpose of development assurance is to identify classes of error that occur during development and to implement mitigations to prevent those errors. Development assurance standards like RTCA DO-278A, RTCA DO-254, and SAE ARP4754A were developed by industry experts sharing experience and mitigation techniques to prevent the most common development mistakes. Development assurance reduces the number of errors in the design because testing will not find every error. For example, to test all possible corner cases[4] of a software program or a programmable hardware device, each decision point would have to be executed using every possible test case combination. This amount of testing is not feasible in complex electronics.

5 Development Assurance Related to Operational Hazards

Designs do not fail in a probabilistic or quantifiable fashion. System failures and malfunctions are due to errors in requirements, design, and implementation. For example, while components may fail, memory may go bad, and resistors may burn out, the design “blueprint” and software code may simply be wrongly designed. These design errors manifest themselves as system errors. To acknowledge failures that result from error, as well as situations in which exhaustive testing of software is impractical or too costly, development assurance methods must be used as a means of approval.

The severity of the hazards to which components may contribute (should that component experience anomalous behavior) determines the specific development assurance objectives

4. A corner case involves a problem or situation that occurs only outside of normal operating parameters.

that must be met. This variation in objectives results in Development Assurance Levels (DALs) based on the severity of these hazards. The higher the specified DAL, the higher the development assurance rigor that must be imposed.

The PO must have a development assurance approach for systems, complex hardware, and software. For systems and complex hardware, the AMS does not recognize a development assurance standard, but the Aircraft Certification Service (AIR) recognizes SAE ARP4754A and RTCA DO-254. For ground software, the AMS recognizes the development assurance guidance provided by RTCA DO-278A as an approval means. AIR recognizes software development assurance guidance provided by RTCA DO-178C as a certification means for airborne software.

5.1 Determining DALs

Determining the software DAL[5] related to a hazard involves the following steps:

- Determine a hazard's severity classification (see Section 5.1.1).
- Assign the DAL in accordance with the severity classification (see Section 5.1.2).
- Determine whether architectural considerations warrant a DAL different from the initial Assurance Level (AL) (see Section 5.1.3).

5.1.1 Determining a Hazard's Severity Classification

Severity is the consequence or impact of a hazard's effect or outcome in terms of degree of loss or harm. It is a prediction of how adverse or serious a particular outcome of a hazard will be. Hazard severity is classified according to the outcome expected to result from the occurrence of that hazard. In accordance with the SMS Manual, the following severity classifications are recognized for ground systems, including software:

- Catastrophic
- Hazardous
- Major
- Minor
- Minimal

In determining severity, some factors to be considered include:

- Airspace requirements, such as:
  - Separation minima,
  - Required navigation performance,
  - Required communication performance,
  - Altitude restrictions, and
  - Obstacle clearance minima;
- Aircraft requirements;
- Procedural requirements;

5. RTCA DO-278A uses the terms "software assurance level" and "Assurance Level," denoted by the abbreviation "AL" to signify "software DAL." RTCA DO-178B and RTCA DO-178C use the term "software level" to signify "software DAL." Regardless of the differences in terminology between these documents, "DAL," "AL," and "level" convey the same concept.

- System state / flight phases; and
- Nominal/off-nominal conditions.

The SMS Manual provides guidance for determining the severity classification to assign to a hazard.

5.1.2 Assigning a DAL in Accordance with a Hazard's Severity Classification

A DAL must be assigned according to the severity of the hazard to which the component may contribute should that component experience anomalous behavior. For software, the relationships between the ALs from RTCA DO-278A and the ATO SMS hazard severity classifications are shown in Table J.1.

Table J.1: Relationships between ATO SMS Hazard Severity Classifications and Software ALs

Hazard Severity Classification	Software ALs According to RTCA DO-278A
Catastrophic	AL1 applies to software whose anomalous behavior would cause or contribute to a failure or malfunction resulting in catastrophic hazard severity.
Hazardous	AL2 applies to software whose anomalous behavior would cause or contribute to a failure or malfunction resulting in hazardous hazard severity.
Major	AL3 applies to software whose anomalous behavior would cause or contribute to a failure or malfunction resulting in major hazard severity.
Not Assigned	AL4 is not associated with or equivalent to any hazard severity classification.
Minor	AL5 applies to software whose anomalous behavior would cause or contribute to a failure or malfunction resulting in minor hazard severity.
Minimal	AL6 applies to software whose anomalous behavior would cause or contribute to a failure or malfunction resulting in either minimal hazard severity or no safety effect.

5.1.3 Architectural Mitigation

Component partitioning is key to architectural mitigation. An entire system can be designed as one partition or many partitions. Two components (hardware or software) can be partitioned if they do not share components or data. This is also referred to as independence. Software can also be partitioned based on timing if two components do not share data and never share the same resources at the same time. If two components are partitioned, then they cannot affect each other.

A DAL is assigned to each partition based on the worst hazard it can cause. Components that can affect each other can be in the same partition and have the same DAL. Since DALs have different levels of rigor, it is cost effective to minimize the number of components in the most rigorous DAL partition and maximize the number of components in the least rigorous DAL partition. In some cases, architectural mitigation may justify a revision of the DAL to a less stringent classification. Guidance for architectural mitigation can be found in RTCA DO-278A, Section 2.4, *Architectural Considerations*, and SAE ARP4754, Section 5.2.3.

6 Software Considerations and the Use of RTCA DO-278A

This section provides guidance for developing software in Communication, Navigation, and Surveillance (CNS) and Air Traffic Management (ATM) systems and equipment in accordance

with RTCA DO-278A. RTCA DO-278A provides an acceptable means of approval for CNS/ATM systems and equipment software by establishing an assurance process that:

- Demonstrates that the CNS/ATM software performs its intended function;
- Minimizes the possibility of software errors;
- Verifies that the software correctly implements its specified requirements;
- Demonstrates traceability to specified higher-level requirements; and
- Demonstrates that the CNS/ATM software, as installed in the target system, supports the airborne systems and equipment compliance to the regulations.

This assurance process includes objectives and activities for planning, development, verification, quality assurance, Configuration Management (CM), and approval authority coordination. It also includes rigorous, iterative, and structured objectives and activities by which CNS/ATM software should be developed. Each objective is supported by a recommended set of activities. Each AL identifies applicable objectives and the level of independence required.

The assurance process identifies a defined set of interrelationships, sequencing, independence, configuration control, feedback mechanisms, and transition criteria. Throughout the assurance process, the software requirements are traced and verified to assure system/software functionality and compliance with safety objectives and requirements.

6.1 Software DALs

Within the safety risk assessment process, safety-related requirements are employed to reduce the residual risk of the acquired system. For software, a DAL is assigned according to the severity of the hazard to which the software may contribute should that software experience anomalous behavior. RTCA DO-278A defines six software DALs: AL1 through AL6. How these ALs apply is described below:

- AL1 applies to CNS/ATM software that must satisfy the most stringent objectives and is analogous to RTCA DO-178C airborne software level A.
- AL2, AL3, and AL5 apply to CNS/ATM software that satisfies successively less stringent objectives and are analogous to RTCA DO-178C airborne software levels B, C, and D, respectively.
- AL4 applies to CNS/ATM software that satisfies objectives less stringent than AL3 but more stringent that AL5. AL4 is not consistent with or equivalent to any RTCA DO-178C airborne software levels.
- AL6 applies to CNS/ATM software whose anomalous behavior, as determined by a safety assessment process, cannot cause or contribute to a failure of system function resulting in a safety impact and is analogous to RTCA DO-178C airborne software level E.

As described above and as displayed in Table J.2 below, the CNS/ATM software DALs specified in RTCA DO-278A correlate with the software levels specified in RTCA DO-178C — except at RTCA DO-278A AL4, where there is no corresponding RTCA DO-178C software level. To promote harmonization between the airborne and CNS/ATM standards, a consistent approach to the selection of software DAL is required when aircraft safety may be

affected. Therefore, any inconsistencies between the applications of the two guidance documents must be rectified.

CNS/ATM software may be justified to AL4 when there is no failure effect on airborne systems. However, when the safety assessment requires RTCA DO-178C development to Level C, and the CNS/ATM software may cause a potential hazard to the aircraft such as message corruption, then the CNS/ATM software must be developed to at least AL3. This is necessary to instill an acceptable level of confidence that an anomaly in the CNS/ATM software will not result in unacceptable behavior of the airborne system.

Table J.2: Correlation of CNS/ATM ALs and Airborne Software Levels

RTCA DO-278A AL	RTCA DO-178C Software Level
AL 1	A
AL 2	B
AL 3	C
AL 4	No Equivalent
AL 5	D
AL 6	E

6.2 Commercial Off-the-Shelf Software

The use of Commercial Off-the-Shelf (COTS) software has been widely adopted in software development projects for CNS/ATM systems and equipment. Examples of COTS software include operating systems, real-time kernels, user-interface software, application software/configuration items, communication and telecommunication protocols, runtime libraries, and data management systems. COTS software can be purchased alone or in conjunction with COTS hardware—such as workstations and communication and network equipment—or hardware items such as memory, storage, and input/output devices. There may be instances in which the use of COTS software is impractical to avoid, such as when a library code is associated with certain compilers. It is essential that the level of confidence for COTS software be the same as for any other software used along a CNS/ATM systems and equipment chain. RTCA DO-278A in its entirety provides a means for evaluation and acceptance of CNS/ATM software. In particular, RTCA DO-278A, Section 12.4, *Commercial Off-the-Shelf Software*, describes the framework for COTS compliance and approval. This framework includes:

- Additional objectives for COTS software lifecycle processes,
- A description of activities and considerations for achieving those objectives,
- A description of evidence that demonstrates that the objectives have been met, and
- Some alternative strategies to provide assurance for COTS software that may have only partial (or no) evidence of compliance with the RTCA DO-278A objectives.

6.3 Legacy Systems

The legacy NAS and the associated developmental processes in place prior to March 14, 2005, were accepted as a baseline prior to the transition to the SMS. Any changes to the NAS after the establishment of the baseline must be SMS compliant; therefore, any change to the NAS baseline software after March 14, 2005, must be (1) considered for its contribution to identified

hazards in accordance with the SMS and, if appropriate, (2) developed and verified in accordance with RTCA DO-278A.[6]

Unaffected portions of NAS baseline software do not need to comply with the RTCA DO-278A objectives. Unaffected portions are those that are neither changed nor affected by changes, as determined by control flow, data flow, memory usage, or timing analysis. The safety analysis should determine the affected and unaffected portions.

Software development and verification tools used for the baseline software may need to be qualified in accordance with RTCA DO-278A.

6.4 Reuse of Previously Approved Software in a CNS/ATM System

RTCA DO-278A, Section 12.1.2, *Reuse of Previously Approved Software in a CNS/ATM System*, addresses CNS/ATM systems or equipment containing legacy software that has been previously approved. The system safety assessment process evaluates the new CNS/ATM system and determines the required AL.

The following describe the circumstances addressed in RTCA DO-278A with respect to previously developed software and reuse:

- If the previously approved software complies with the RTCA DO-278A objectives, there are no changes to the software, and the AL is the same for the new system, then no additional effort is required.
- If modifications are to be made to the previously approved software, the guidance established in RTCA DO-278A, Section 12.1.1, *Modifications to Previously Developed Software*, must be satisfied.
- If the software lifecycle data from a previous application are inadequate or do not satisfy the objectives for the new application, the guidance in RTCA DO-278A, Section 12.1.4, *Upgrading a Development Baseline*, must be satisfied.

6.5 Software Tool Qualification

Qualification of a software tool is necessary when RTCA DO-278A software processes are being eliminated, reduced, or automated by use of the tool without the tool's output being verified as specified in RTCA DO-278A, Section 6, *Software Verification*. RTCA DO-278A defines a software tool as "a computer program used to help develop, test, analyze, produce, or modify another program or its documentation." Examples of some software tools include, but are not limited to, the automatic source code generator, structural coverage analysis, and software standards checkers.

RTCA DO-278A, Section 12.2, *Tool Qualification*, provides guidance on applying development assurance to software tools and on how to determine the Tool Qualification Level (TQL). In addition, RTCA DO-330 provides objectives, activities, guidance, and lifecycle data required for each TQL.

6.6 Service Experience

RTCA DO-278A, Section 12.3.4, *Service Experience*, provides guidance for determining whether equivalent safety for software can be demonstrated by the software's product service

6. In rare cases, this requirement may be waived. Contact Safety and Technical Training (AJI) Policy and Performance, AJI-3, for more information.

experience and addresses approval credit that may be granted when this is the case. Some primary considerations include:

- The relevance of service experience, such as time in service, CM, how the software was used, and the relevance of the environment in which it was used;
- The adequacy of problem reporting to the level that any software failures during the service period were appropriately reported, recorded, and resolved; and
- The stability and maturity of the software, including effects of any changes during the service period.

6.7 Alternative Methods

An applicant may propose an alternative method of approval to RTCA DO-278A. When proposing alternative methods of approval, applicants should consult FAA AC 20-171. Although AC 20-171 addresses alternatives to RTCA DO-178B, the guidance can be used for proposing alternative methods to RTCA DO-278A for CNS/ATM software.

When proposing a method of approval that is alternative to RTCA DO-278A, the applicant must:

- Identify a compliance approach that addresses the principles described in this guidance and describe how the alternative approach meets the intent of the objectives and/or activities defined in the RTCA DO-278A process-based approach.
- Show that the proposed alternative demonstrates a level of safety assurance equivalent to AMS, Section 4.12. RTCA DO-278A establishes a level of safety assurance for software components that supports the demonstration of compliance to AMS, Section 4.12.
- Thoroughly document the proposed alternative approach and rationale.
- Obtain agreement from the ATO Chief Safety Engineer that the proposed approach meets the original intent of the objectives and/or associated activities.
- Provide substantiating evidence to the approval authority, demonstrating that the agreed-upon approach was followed.

6.8 Approval Process

The DAL is determined through the safety assessment process. The assessment validates that the appropriate DAL has been assigned to the correct safety hazards and allocated to the correct safety requirements. Policy and guidance for approving safety assessments for acquisitions affecting the NAS are detailed in the SMS Manual.

Detailed guidance for the approval process related to RTCA DO-278A lifecycle data is provided in Appendix L and can also be obtained through consultation with the approval authority.

Uncontrolled copy when downloaded

7 Product Development in the AMS Lifecycle

7.1 Service Analysis and Strategic Planning / Concept and Requirements Definition

Planning for development assurance needs to begin early in the AMS lifecycle so the DAL can be factored into the business case. Typically, this occurs prior to the Investment Analysis Readiness Decision while the Operational Safety Assessment (OSA) is being developed. The DAL is initially established from the OSA and is included in the preliminary Program Requirements Document (PRD). More information on Service Analysis and Strategic Planning or Concept and Requirements Definition is available on the FAA Acquisition System Toolset (FAST) website.

7.2 Investment Analysis

The DAL is validated in the Comparative Safety Assessment, which may differ between investment alternatives. The DAL for the alternatives is then included in the business case and Implementation Strategy Planning Document (ISPD) prior to the Initial Investment Decision.

The final DAL is determined from the Preliminary Hazard Analysis. This final DAL is included in the final PRD and Program Safety Plan (PSP). Any changes to the DAL are included in the final versions of the business case and ISPD prior to the Final Investment Decision. More information on the Investment Analysis is available on the FAST website.

7.3 Solution Implementation

Prior to contract award, the DAL is established based only on functional requirements. After the initial establishment of the DAL and contract award are completed, the developer performs hazard assessments in accordance with the contract. It is important to validate that the appropriate DAL has been assigned to each safety hazard and allocated to the correct safety requirements after the developer hazard assessments are performed and after any change in system requirements.

It is critical to provide development assurance oversight throughout Solution Implementation (SI) because various objectives must be met during this phase. Noncompliance discovered late will require rework, resulting in cost and schedule overruns. The PSP should identify intervention points and monitoring objectives to ensure the developer is meeting development assurance requirements. More information on SI is available on the FAST website.

Appendix K

Conducting an RTCA DO-278A Software Assurance Compliance Analysis for Acquired National Airspace System Systems

Conducting an RTCA DO-278A Software Assurance Compliance Analysis for Acquired National Airspace System Systems

1 Purpose

This appendix describes a methodology for evaluating the software assurance compliance of National Airspace System (NAS) systems[1] being acquired in accordance with the Federal Aviation Administration (FAA) Acquisition Management System (AMS) when one of the following applies:

- An RTCA[2] DO-278−compliant system is being upgraded per RTCA DO-278A guidance.[3]
- A system is being developed and evaluated under RTCA DO-278A guidance.
- A system is being developed and evaluated under guidance other than RTCA DO-278A.

The result of this evaluation is a software assurance compliance analysis.

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in FAA orders. It supplements and reflects updates to the Air Traffic Organization (ATO) Safety Management System (SMS) Manual, which provides guidance on fulfilling requirements set forth in the current version of FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements FAA AMS policy.

The primary reference materials in this appendix are the current editions of the following:

- AMS, Section 4.12, *National Airspace System Safety Management System*;
- SMS Manual;
- FAA Order JO 1000.37; and
- The following RTCA documents:
    - RTCA DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*;
    - RTCA DO-248C, *Supporting Information for DO-178C and DO-278A*;
    - RTCA DO-330, *Software Tool Qualification Considerations*;
    - RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A*;
    - RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*; and
    - RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*.

3 Background

RTCA DO-278A provides guidance for the production of software contained in non-airborne Communication, Navigation, and Surveillance (CNS) and Air Traffic Management (ATM)

1. This may include major system modifications that are treated as new acquisitions.

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

3. An RTCA user identity and password are required to download RTCA documents. FAA employees may obtain an RTCA membership by contacting RTCA.

systems. It is the ATO's intent that all new non-airborne systems and modified legacy systems treated as new acquisitions in the NAS are developed in accordance with RTCA DO-278A.

The Program Office (PO) must conduct a software assurance compliance analysis for each component of a system going through the AMS process that contains software. If the program involves legacy software components that were not developed to the requirements of RTCA DO-278A, the PO must conduct a compliance gap analysis for each component of a modified legacy system that contains software. A vendor may choose to submit to the PO a self-assessed compliance gap analysis on one of the existing products in support of the contract award.

The only difference between a software assurance compliance analysis and a compliance gap analysis is that the gap analysis is conducted on a previously completed project to ensure a program's work will pass future compliance evaluations, and the compliance analysis is conducted on a new product while it is being developed. The purpose of the gap analysis is to update a system developer's processes and identify specific activities that must be addressed to ensure the processes and product are compliant.

It is important to note that many of the non-airborne CNS/ATM systems currently in the NAS were developed and fielded using integrity assurance guidelines other than those contained in RTCA DO-278A. Reasons for having used alternative guidelines include:

- RTCA DO-278A was not yet developed or was not yet widely accepted, and the system developers / subcontractors did not conduct safety analyses for the software components of the system.
- Other software development standards (e.g., DOD-STD-2167A, MIL-STD-498, EIA 12207, or FAA-STD-026A) were used to implement the software development process.
- RTCA DO-178 (the airborne systems equivalent of RTCA DO-278) was used to evaluate the development of non-airborne CNS/ATM systems.

If systems previously developed/fielded using alternative guidelines are modified under a new acquisition, the PO must evaluate new and affected software for compliance with RTCA DO-278A.

4 Compliance with the Standard

RTCA DO-278A was developed by the aviation industry and contains guidance and best practices for developing software. This section describes the nature of content in RTCA DO-278A and how to use the guidance therein when identifying requirements.

4.1 RTCA DO-278A Guidance and Objectives

4.1.1 Objective Guidance

Objective guidance is specific, and compliance to this guidance can be easily observed during audit activities. Ensuring compliance to objective guidance is done by identifying evidence that a requirement has been satisfied. For example, if the guidance requires each configuration

item[4] and its successive versions to be labeled unambiguously, then ensuring compliance would simply involve verifying that each item has an unambiguous configuration identifier.

4.1.2 Subjective Guidance

Subjective guidance is not as specific as objective guidance, and compliance to this guidance is not as easily observed or audited. Compliance to subjective guidance cannot be verified directly; it must be demonstrated through performance.

4.1.3 Top-Level Objectives

Top-level objectives were developed as a way to identify what content is required for the different Development Assurance Levels (DALs). Each top-level objective is a summary of many sub-objectives. Complying with a top-level objective demonstrates compliance with all the guidance within that objective's category. For example, in RTCA DO-278A, one top-level objective is to define the activities of the software lifecycle processes. There are over one hundred paragraphs describing the different aspects of lifecycle processes; each aspect would need to be accounted for / defined in the system's/company's lifecycle process activities in order to satisfy the associated top-level objective.

4.1.4 Administrative Content

Some text within RTCA DO-278A exists only for introductory or administrative purposes (like headings and notes) and is not considered guidance. It is not required to provide evidence of compliance with this type of content.

4.2 Identifying Requirements

The system developer must review all the content in RTCA DO-278A, identify which paragraphs are guidance / communicate requirements, and map these paragraphs to specific top-level objectives. This will help simplify future software assurance compliance analyses / compliance gap analyses.

5 Procedures

The PO (with support from the Program Safety Team, when applicable) must follow the process outlined below to perform an RTCA DO-278A software assurance compliance analysis and document its results.[5] The ATO SMS Toolbox provides compliance analysis tools that can be used for documenting the results and collecting the proper evidence for the compliance evaluation. Regardless of whether a program uses ATO-provided analysis tools or other means, the steps detailed in this section must be followed.

5.1 Establish the Software DAL Allocations

Perform a System Safety Analysis to determine whether the existing system architecture satisfies safety requirements.[6] Form the system architecture and allocate safety requirements to the software. Then, establish the appropriate DAL[7] for all partitions of the CNS/ATM system. Once the DALs are established, start the RTCA DO-278A software assurance compliance analysis for each DAL.

---

4. A configuration item is a component of a system that can be identified as a self-contained unit for purposes of change control and identification.

5. As a program moves through the AMS lifecycle, program management responsibilities transfer from the Office of NextGen to Mission Support Services, the Program Management Organization, or Technical Operations.

6. The SMS Manual contains more information on performing a System Safety Analysis.

7. "DAL" conveys the same concept as "Assurance Level (AL)" (used in RTCA DO-278A) and "software level" (used in RTCA DO-178C).

5.2 Establish a Document/Process Baseline

Most companies do not use the same titles for requirements documents. With the active participation of the system developer / subcontractor whose system/software is being evaluated, identify all company documents / data items that will satisfy the required data items in RTCA DO-278A, RTCA DO-330, RTCA DO-331, RTCA DO-332, and RTCA DO-333. This information must be used to determine the system developer's / subcontractor's existing lifecycle data baseline, which must be aligned with RTCA DO-278A lifecycle data requirements (including applicable supplements) for each DAL. Also, identify the program, safety, and system documents that a developer/subcontractor has produced or will need to provide/develop for the new and/or modified system; and identify any document and/or process that is not applicable to the program. RTCA DO-278A provides outlines for the 22 different data items. It is important to identify where this data content exists in the company documents. (For example, the content required in one RTCA DO-278A document may be distributed through multiple existing company documents. It would be important to identify all documents that contain this content so it can be easily found.)

According to RTCA DO-278A, Section 7.3, software lifecycle data can be assigned to one of two Configuration Management (CM) Control Categories (CCs) according to the associated activities required for Software CM. (Activities associated with CC2 data are a subset of CC1 activities. These CCs are further delineated within Section 7.3 of RTCA DO-278A as well as in Annex A of the same document.) Even new developments must identify every planned release of CC1 and CC2 lifecycle data and must decide how the documents containing these data will be identified (e.g., what configuration code, title, or other identifier will be used for each document). This listing of planned documents is a content requirement for the Plan for Software Aspects of Approval (PSAA). The listing of all finalized documents and their identifiers is a content requirement for the Software Configuration Index (see Appendix M).

5.3 Determine Documentation Needs

Request the appropriate documents from the system developer / subcontractor and other sources and conduct on-site visits for reviews or follow-up activities, as required. Compare the information gathered to the types of evidence described in RTCA DO-278A. It may be helpful to consider the following items before providing evidence of compliance:

- Previously developed software.
- Alternative methods of acquiring software.
- Commercial off-the-shelf software.

5.4 Develop and Record RTCA DO-278A Evaluation Criteria

For each document used to support software development, identify the specific RTCA DO-278A guidance with which the document will comply. The focus of the compliance evaluation is to identify the evidence in a document that indicates compliance with RTCA DO-278A objectives, recognizing that the software lifecycle data may or may not align with RTCA DO-278A terminology. Capture the evaluation of each RTCA DO-278A objective / guidance paragraph and ensure that the guidance has been satisfied. Identifying what evidence to look for and where it may be found is a significant task. However, providing a general guide for where to find this information can be done in advance and will make this task simpler. The compliance analysis tools on the ATO SMS Toolbox may assist in this, but whether using these tools is appropriate depends on the company's document structure. Assistance from the system developer / subcontractor is invaluable in determining where to locate the desired evidence.

5.5 Have the System Developer / Subcontractor Conduct a Self-Evaluation

Have the system developer / subcontractor evaluate their own software development efforts against the RTCA DO-278A criteria and record the findings. This will help Subject Matter Experts (SMEs) and the compliance evaluation team better understand the document structure, system/software architecture, organization, development processes, and verification approach.

5.6 Identify Evidence of Compliance

Locate the content within the system developer's documents that demonstrates compliance with the RTCA DO-278A guidance. The labeling of the document's contents does not have to match the RTCA DO-278A document descriptions as long as the intent of the text clearly satisfies RTCA DO-278A requirements. CM is required for all developer documents.

5.7 Rate the Level of Compliance with RTCA DO-278A Guidance

Once the system developer / subcontractor has provided the requested documents and process descriptions, review the submissions with the RTCA DO-278A SMEs to determine whether the developer's/subcontractor's submissions align with the RTCA DO-278A guidance. Evaluate compliance to applicable RTCA DO-278A guidance and remember that different guidance may apply to different DALs. Use the identified top-level or sub-objectives (mentioned in Section 4.1.3) as the means to map the guidance to the DALs. Identify the compliance rating as Satisfied (S), Partially Satisfied (P), Not Satisfied (N), or Not Applicable (X) using the following evaluation criteria:

- Satisfied: The RTCA DO-278A guidance has been met through normal means and has been fully satisfied.
- Partially Satisfied: The RTCA DO-278A guidance has been partially met through normal means and its intent has been partially satisfied.
- Not Satisfied: The RTCA DO-278A guidance has not been met through normal means and its intent has not been satisfied.
- Not Applicable: The RTCA DO-330, RTCA DO-331, RTCA DO-332, or RTCA DO-333 guidance is not applicable to this project.

5.8 Evaluate Progress

5.8.1 Justify the Evaluation

Record how the reviewed documentation demonstrates or does not demonstrate compliance with RTCA DO-278A guidance. List the documents, sections, and paragraphs that support the compliance rating or provide a rationale for why the evaluation may be (P) or (N).

5.8.2 Indicate Whether Additional Documents are Needed

Identify additional documents and processes needed to fully evaluate compliance to the RTCA DO-278A guidance.

5.8.3 Summarize the RTCA DO-278A Software Assurance Compliance Analysis

Once compliance to applicable RTCA DO-278A guidance has been evaluated and assigned a compliance rating (see Section 5.7), review the results and summarize the overall findings.

5.8.4 Conduct an Initial Evaluation of Compliance with RTCA DO-330 Tool Qualification Requirements

The RTCA DO-330 supplement is applicable when the system developer / subcontractor has used or plans to use tools for qualified activities. Repeat the prior activities of Section 5.8 to evaluate all Tool Qualification (TQ) objectives for RTCA DO-330 compliance.[8] Provide a discussion for each tool as to its use and TQ need and status.

5.8.5 Conduct an Initial Evaluation of Compliance with RTCA DO-331 Model-Based Development Requirements

The RTCA DO-331 supplement is applicable when the system developer / subcontractor has used or plans to use Model-Based (MB) development. Repeat the prior activities of Section 5.8 to evaluate all MB development objectives for RTCA DO-331 compliance. If this supplement is not applicable, provide a rationale as to why it is not.

5.8.6 Conduct an Initial Evaluation of Compliance with RTCA DO-332 Object-Oriented Techniques

The RTCA DO-332 supplement is applicable when the system developer / subcontractor has used or plans to use Object-Oriented Techniques (OOT). Repeat the prior activities of Section 5.8 to evaluate all OOT objectives for RTCA DO-332 compliance. If this supplement is not applicable, provide a rationale as to why it is not.

5.8.7 Conduct an Initial Evaluation of Compliance with RTCA DO-333 Formal Methods

The RTCA DO-333 supplement is applicable when the system developer / subcontractor has used or plans to use Formal Methods (FM). Repeat the prior activities of Section 5.8 to evaluate all FM objectives for RTCA DO-333 compliance. If this supplement is not applicable, provide a rationale as to why it is not.

5.8.8 Conduct On-Site Visits

After desk reviews have been completed, the evaluation team should schedule visits to the system developer's / subcontractor's facilities to review additional documents/processes, interview key personnel, and complete any remaining fields of the worksheet. During this time, the RTCA DO-278A, RTCA DO-330, RTCA DO-331, RTCA DO-332, and RTCA DO-333 evaluations may be updated and re-evaluated based on the additional documents and interviews.

5.8.9 Identify Corrective Actions

For all findings of noncompliance, the system developer must identify corrective actions for bringing the development into compliance. If a finding of noncompliance is discovered after the lifecycle data has been documented (e.g., in a gap analysis of a legacy product or late in a development), the developer must analyze the non-compliance and take remedial actions to correct any identified problems.

5.9 Produce a Final Software Assurance Compliance Analysis or Compliance Gap Analysis Report

Produce a final report containing the RTCA DO-278A software assurance compliance analysis or the compliance gap analysis and include a description of further actions required to correct any identified noncompliance.

8. The TQ process is referenced in RTCA DO-278A in Section 12.2 and Table A-1, Objective 4. Additional guidance for TQ can be found in RTCA DO-330.

For a compliance gap analysis, the PSAA must address how the RTCA DO-278A gaps found during the evaluation will be resolved and how the gap resolution process will fit into the software development process. If the PSAA is not available or the current plan is found inadequate through the compliance gap analysis, the PO must request that the system developer / subcontractor either develop a new plan or update the current plan. The PSAA must also include the gap analysis as part of its documentation.

For a compliance analysis, a report should be generated with each review of the project and submitted for internal company safety approval. (See Appendix L for the four typical reviews.) The system developer must develop a report of the noncompliance findings, and noncompliance issues must be resolved before the Software Accomplishment Summary can be completed. These reviews are the evidence of compliance that will permit the approval authority to sign the System Safety Assessment Report.

Appendix L

Software Assurance Approval Guidelines for Communication, Navigation, Surveillance and Air Traffic Management Systems

Software Assurance Approval Guidelines for Communication, Navigation, Surveillance and Air Traffic Management Systems

1 Purpose

This guidance describes how to demonstrate adherence to applicable objectives from RTCA[1] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*.

2 Applicable Policy and Related Documents

This appendix does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the Air Traffic Organization (ATO) Safety Management System (SMS) Manual, which provides guidance on fulfilling requirements set forth in the current version of FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. This appendix also supplements FAA Acquisition Management System (AMS) policy.

The primary reference materials in this guidance are the current editions of the following:

- AMS, Section 4.12, *National Airspace System Safety Management System*;
- SMS Manual;
- FAA Order JO 1000.37;
- FAA Order 8100.8, *Designee Management Handbook*; and
- The following RTCA documents:[2]
    - RTCA DO-278A;
    - RTCA DO-248C, *Supporting Information for DO-178C and DO-278A*;
    - RTCA DO-330, *Software Tool Qualification Considerations*;
    - RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A*;
    - RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*; and
    - RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*.

3 Background

AMS, Section 4.12, requires that a software product be developed at a rigor commensurate with the severity of the associated hazard, should that product experience a failure. For software-intensive systems, the establishment of a development assurance program in accordance with RTCA DO-278A is an acceptable (but not the only) means of demonstrating that a software product was developed at the appropriate level of rigor. RTCA DO-248C provides clarification on the guidance material in RTCA DO-178C and RTCA DO-278A and should be used as a companion document when seeking additional information. References to RTCA DO-178C are provided for comparison, since these considerations concern airborne systems. RTCA DO-330 is a standalone document that provides software Tool Qualification (TQ)

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

2. An RTCA user identity and password are required to download RTCA documents. FAA employees may obtain an RTCA membership by contacting RTCA.

guidance, and it is applicable when software tools must be qualified per the guidance in RTCA DO-278A.

When using RTCA DO-278A as a means of ensuring compliance with AMS, Section 4.12, the associated RTCA DO-278A supplements must also be used where applicable. RTCA DO-331, RTCA DO-332, and RTCA DO-333 are supplements that address certain software development techniques and can add, delete, or modify objectives, activities, and lifecycle data in RTCA DO-278A. Guidance within a particular supplement must be applied when using the addressed technique. The Plan for Software Aspects of Approval (PSAA) must identify applicable supplements and describe the intended use of each.

RTCA DO-278A establishes an approval liaison process that has similarities to the RTCA DO-178C certification liaison process for aircraft software. However, there are also fundamental differences to be considered. In the case of aircraft, the applicant is external to the FAA and is regulated by the certification authority. In the case of Communication, Navigation, and Surveillance (CNS) and Air Traffic Management (ATM) systems, the applicant is internal to the FAA while the software developers are external. If it is determined through safety analyses that the CNS/ATM software can affect systems onboard an aircraft, the assigned Development Assurance Level must be acceptable to the aircraft certification authority. The certification authority must also be allowed to provide input to the approval process.

4 Definitions

RTCA DO-278A and some other standards use terms that have different definitions than those used in the AMS. For the purposes of this appendix, these definitions apply:

- An **applicant** is the organization that is the primary sponsor of the system. The applicant is usually responsible for acquiring a new system or proposing changes to an existing system, and for asking the approval authority for permission to deploy the system. For AMS programs, the applicant is typically the Program Office (PO).
- The **approval authority** is the organization that is responsible for approving the safety aspects of the system (but not the funding or functionality unless that functionality affects the safety of the system). The ATO authority that accepts and/or approves the safety aspects of CNS/ATM systems that affect the National Airspace System is the ATO Chief Safety Engineer.

  Note: Approving software lifecycle data (as defined in this appendix) is the method of providing RTCA DO-278A compliance substantiation. It does not replace established processes related to FAA acceptance of software.
- The **certification authority** is the aviation authority that accepts and/or approves software lifecycle data for aircraft.
- A **configuration item** is (1) one or more software components treated as a unit for software Configuration Management (CM) purposes or (2) software lifecycle data (i.e., documentation) treated as a unit for software CM purposes.
- A **developer** is usually the prime contractor for the system under development and is responsible for system integration.

Uncontrolled copy when downloaded

- A **finding** traces to a specific RTCA DO-278A objective and conveys both positive and negative comments that relate to how the developer is meeting the intent of that objective.
- **Issue papers** are a means of documenting technical and approval issues that must be resolved before approval. Final meeting minutes are an acceptable form of documentation.
- **Reuse** is the subsequent use of unaffected, previously approved software lifecycle data.
- **Review** is the act of inspecting or examining software lifecycle data, software project progress and records, and other evidence to assess compliance with RTCA DO-278A objectives. A review may involve a combination of reading documents, interviewing project personnel, witnessing activities, sampling data, and participating in briefings. Reviews may be conducted at one's own desk, at a developer's facility, or at the facility of the developer's supplier.
- An **RTCA DO-278A Compliance Gap Analysis** is an analysis tool/process used to evaluate a developer's current RTCA DO-278A or non–RTCA DO-278A software processes/practices to determine how the applicant/developer complies with RTCA DO-278A guidance. For additional information on conducting an RTCA DO-278A Compliance Gap Analysis, see Appendix K.
- **Sampling** is selecting a representative set of software lifecycle data for inspection or analysis. The purpose of sampling is to determine the compliance of all software lifecycle data in the project developed up to that point in time. Sampling is the primary means of assessing the compliance of the software processes and data. Examples of sampling may include:
    - Inspecting the traceability from system requirements through software requirements, software design, source code, object code, test cases and procedures, and test results;
    - Reviewing analyses used to determine system safety classification, Assurance Level (AL), or RTCA DO-278A compliance;
    - Examining the structural coverage of source code modules; and
    - Examining Software Quality Assurance (SQA) records and CM records.
- A **software configuration library** is a controlled repository of software and related data as well as documents designed to aid in software development, use, or modification.
- **Software lifecycle data** are data produced during the software lifecycle that are used to plan, direct, explain, define, record, or provide evidence of activities.
- **Software plans and standards** are data products that direct software development and associated processes.
- A **subcontractor** can be the developer, verifier, or individual otherwise involved with the development of the software. The subcontractor reports to the prime contractor.
- A **Subject Matter Expert (SME)** has qualified skills and knowledge related to software assurance, specifically to RTCA DO-178C and RTCA DO-278A. An RTCA

Uncontrolled copy when downloaded

DO-178C–designated engineering representative is considered a qualified RTCA DO-278A SME. FAA Order 8100.8 provides details on RTCA DO-178C qualifications.

5 Roles and Responsibilities

This section discusses the safety responsibility for each role specific to development assurance. Though this section specifically addresses software, the same approach applies to system and hardware development assurance activities.

5.1 System Developer

The system developer is responsible for implementing the system requirements. The developer performs development engineering and—through a process of checks and balances and various methods and techniques—produces a product that has sufficient rigor commensurate with the severity of the system. For an RTCA DO-278A project, the breakdown of responsibilities within the developer's organization tends to be as follows:

- Engineering management must develop an approach on how the team will comply with standards. This approach must be captured in the five software plans and three software standards discussed in RTCA DO-278A, Sections 11.1 through 11.8.
- Software engineering must utilize the processes, methods, and tools identified in the plans and standards and produce a product that implements the system specifications. If these specifications are followed, the system should be compliant with RTCA DO-278A.
- SQA must oversee software engineering through a series of reviews and audits to ensure they are following the plans and comply with all requirements, which include those of RTCA DO-278A, the system specifications, and any other standards. The results of these activities are captured using CM, and they become evidence of compliance.

5.2 Applicant

The applicant, which is typically the PO, is responsible for verifying that the developer complies with RTCA DO-278A, the system specifications, and any other standards. The applicant must do so by:

- Producing a Program Safety Plan (PSP) that describes all the reviews, checklists, and activities the applicant will perform to ensure the developer complies with RTCA DO-278A;
- Ensuring the contract contains the development assurance requirements with which the developer must comply;
- Performing reviews and audits of the developer's SQA activities;
- Spot-checking the software engineering products to verify SQA's work;
- Approving all software documentation generated by the developer; and
- Submitting evidence of compliance to the approval authority.

It is important to realize that RTCA DO-278A is not just a safety standard. It also is a product approval standard, as it provides for the submittal of a significant amount of documentation that ensures all requirements—not just the safety requirements—have been implemented.

Reviewing these documents will permit the PO a look at how the program is progressing long before the first software build.

5.3 Approval Authority

The approval authority is responsible for approving the safety aspects of the project by leveraging the work done by the applicant. The approval authority does not approve only the software, but the entire system, which includes software, hardware, procedures, and processes. To address the safety requirements related to software development assurance, the approval authority must:

- Review and approve the PSP to ensure that the proposed processes will be sufficient for generating evidence of compliance with RTCA DO-278A,
- Review the evidence of compliance submitted by the applicant,
- Perform audits on the project, and
- Make a finding of compliance with evidence supporting that the RTCA DO-278A standard has been followed.

The approval authority does not review the entire project; they only spot check the evidence to ensure the applicant is fulfilling their responsibilities. It is possible for the approval authority to make a finding of compliance to a program that is not fully compliant. Only the applicant has the visibility and responsibility to ensure the developer's compliance.

The ATO Chief Safety Engineer, as the safety approval authority, allows the PO to review all RTCA DO-278A (or equivalent) deliverables and submit evidence of their compliance reviews. The ATO Chief Safety Engineer will base his/her approval on the evidence of compliance presented and will, as needed, ask to see specific documents as part of the evaluation. The PSP must document the details of this relationship.

6 Software Review Process

The software review process is the vehicle for establishing communication and understanding between the applicant and the approval authority. The review process includes inspection and examination of the software lifecycle data, software project progress and records, and other evidence to assess compliance with RTCA DO-278A objectives. This process may consist of a combination of reading documents, interviewing project personnel, witnessing activities, sampling data, and participating in briefings. RTCA DO-278A, Section 10, states that the approval authority may review the software lifecycle processes and data to assess compliance with RTCA DO-278A. This appendix does not change the intent of RTCA DO-278A but clarifies its application.

6.1 Objectives of the Software Review Process

The 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 whether a project will meet the approval requirements and RTCA DO-278A objectives 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 requirements and supporting data;
- Objective evidence showing that the software project adheres to its approved software plans and procedures; and
- The opportunity for the approval authority to monitor SME activities.

6.2 Interaction between the Software Review Process and the Software Lifecycle

The review process should begin early in the software lifecycle, as this will mitigate the risk of the software / planning decisions not satisfying RTCA DO-278A objectives. Beginning the review process early requires timely communication between the applicant and the approval authority about planning decisions that may affect the software processes and product.

The development of software for a CNS/ATM system may take several months or years. Since RTCA DO-278A is process-oriented guidance, the review process must be integrated throughout the software lifecycle to be meaningful. This means that there should be regular contact between the applicant and the approval authority. Regular contact between the applicant and the approval authority assures both parties that the software development is meeting the required RTCA DO-278A objectives. The four types of recommended reviews are software planning reviews, software development reviews, software verification reviews, and final approval software reviews.

6.2.1 Software Planning Review

Although the software planning process may continue throughout the software lifecycle and plans and standards may change as the project progresses, the planning process is generally considered complete when the associated initial transition criteria are satisfied. The software planning review should take place at this time. Typical criteria for completion of the software planning process include:

- Software plans and standards have been internally reviewed based on company-specified criteria, and all deficiencies have been resolved.
- Software plans and standards have been evaluated by an SQA team, and all deficiencies have been resolved.
- Software plans and standards have been approved and placed under configuration control.
- Objectives 1 and 2 of RTCA DO-278A, Annex A, Table A-1 and Table A-10 have been satisfied.

The applicant or the applicant's SME must make the software plans and standards (shown in Table L.1) available to the approval authority. The supporting software data should undergo the configuration control appropriate for the software AL.

Table L.1: Data Availability 1 for Software Planning Review

Software Data	RTCA DO-278A Section
PSAA (must be submitted to the approval authority)	11.1
Software Development Plan	11.2
Software Verification Plan	11.3
Software CM Plan	11.4

Uncontrolled copy when downloaded

SQA Plan	11.5
Software Requirements, Design, and Code Standards	11.6, 11.7, and 11.8
Software CM Records	11.18
Software Configuration Index (only includes the planning documentation and associated lifecycle data)	11.16
Problem Reports	11.17
SQA Records (as applied to the planning activities)	11.19
Software Verification Results	11.14

Reviewers must also evaluate plans to ensure that all applicable RTCA DO-278A objectives are satisfied when the software plans are followed. Additionally, reviewers must verify that the proposed ALs are in accordance with the hazard severity or severities identified during safety analyses and evaluate the relevance of the software plans and standards to the AL.

6.2.2 Software Development Review

The software development review should be conducted on a sample of the software partway through the development process. The amount of completed software needed and the required sample size will depend on the reviewers' experience with the applicant/developer, the complexity of the program, and other factors. The development data for the selected sample should be sufficiently complete and mature. The following are typical criteria used for identifying a sufficiently mature software sample for the software development review:

- High-level software requirements are documented, reviewed, and traceable to system requirements.
- Low-level software requirements are documented, reviewed, and traceable to high-level requirements.
- The source code implements low-level requirements, is traceable to the low-level requirements, and has been reviewed.
- The software architecture is defined, and reviews and analyses have been completed.

For a software development review, a list of the available software development (verification) artifacts must be agreed upon and documented such that the complete set of data items are reviewed and will be made available to the approval authority and/or RTCA DO-278A SME. The supporting software data should undergo the configuration control that is appropriate for the AL and is in accordance with the approved plans and procedures. The plans listed in Table L.1 should also be provided to the review team before the review.

The objectives applicable to software development in RTCA DO-278A (in Annex A and Tables 12-2 through 12-5) for commercial off-the-shelf software should be used as the evaluation criteria for the software development review. Additionally, the software lifecycle data should be evaluated to determine the effectiveness of the applicant's implementation of the plans and standards in the development process.

6.2.3 Software Verification Review

The software verification review should be conducted on a sample of the software partway through the software development lifecycle process. The amount of completed software needed and the required sample size will depend on the reviewers' experience with the applicant/developer, the complexity of the program, and other factors.

The development data for the selected sample should be sufficiently complete and mature. The following are typical criteria for identifying a sufficiently mature software sample for the software verification review process:

- Development data (e.g., requirements, designs, trace data, the source code, the object code, linking and loading data, and executable images) are complete, have been reviewed, and are under configuration control.
- Test cases and procedures have been documented, reviewed, and placed under configuration control.
- Test cases and procedures have been executed.
- Completed test results have been documented as agreed in the planning documents.
- The software testing environment (including TQ, as required) has been documented and is controlled.

For the software verification review, a list of the available software development (verification) artifacts must be agreed upon and documented such that the complete set of data items are reviewed and made available to the approval authority and/or SME. The supporting software data should undergo the configuration control that is appropriate for the AL and is in accordance with the approved plans and procedures. The data listed in Table L.1 should also be available during the verification review.

The objectives that apply to verification in RTCA DO-278A, Annex A, should be used as the evaluation criteria for the software verification review.

6.2.4 Final Approval Software Review

The final software build establishes the configuration of the software product that the applicant believes complies with all applicable RTCA DO-278A AL objectives. It is the version of the software intended to be used in the approved system or equipment. The purpose of this review is to:

- Determine compliance of the final software product with the appropriate RTCA DO-278A objectives;
- Ensure that all software development, verification, quality assurance, CM, and approval liaison activities are complete;
- Ensure a software conformity review has been completed; and
- Review the final Software Configuration Index (SCI) and Software Accomplishment Summary (SAS). The final approval software review should take place when the software project is completed and satisfies the following criteria:
    - Software conformity review has been performed and any deficiencies have been resolved.
    - The SCI and SAS have been completed and reviewed.
    - All software lifecycle data have been recorded, approved, and placed under configuration control.

For the purposes of this review, all software lifecycle data of RTCA DO-278A must be available

Uncontrolled copy when downloaded

to the approval authority and/or SME. However, only the data shown in Table L.2 are of special interest for this review. The supporting software data should undergo the configuration control appropriate for the AL.

Table L.2: Data Availability for Software Final Approval Review

Software Data	RTCA DO-278A
Software Verification Results	11.14
Software Lifecycle Environment Configuration Index	11.15
SCI	11.16
Problem Reports	11.17
Software CM Records	11.18
SQA Records (including Software Conformity Review Report)	11.19
SAS (must be submitted to the approval authority)	11.20

Evaluation criteria for this review include all objectives of RTCA DO-278A, Annex A. Additionally, all software-related problem reports, action items, approval issues, etc., should be addressed before approval.

Note: Although this appendix proposes four types of reviews, the type, number, and extent of those reviews may not suit every project and applicant. Additional considerations and alternative approaches may be appropriate.

6.3 Intervention Points

The purpose of design assurance is to catch errors as early as possible in the design process and prevent them from being incorporated into the final product. The overall concept is that a review (or intervention) should be conducted:

- Early enough in the design process that corrective action can be taken to ensure compliance and reduce the repetition of work.
- Late enough to have enough data for a good sample to be used to represent how well the development is progressing.
- At a point where progress can be halted, if needed, before the completion of a milestone to resolve issues of non-compliance before they can corrupt the next design stage.

When to conduct each review depends upon the developer's plans. Table L.3 provides a rough timeline of when to conduct the different reviews.

Table L.3: Data Availability for Software Final Approval Review

Software Planning Reviews	Review the draft PSAA as soon as possible. Close out prior to the Preliminary Design Review.
Software Development Reviews	Start after the development of the first draft of the software requirements document. Close out prior to the Critical Design Review.
Software Verification Reviews	Start during software requirements testing. Close out prior to the first delivery of software.
Final Approval Software Reviews	Start prior to formal system-level testing. Close out prior to the physical/functional configuration audit.

To close out a review, each finding of non-compliance should be resolved to prevent errors from further propagating into the product.

6.4 Applicant Involvement

The applicant is responsible for ensuring the developer is compliant with RTCA DO-278A. The applicant, therefore, must conduct all four reviews listed in Table L3. The length and detail of each review is dependent on the AL of the project and the number of non-compliance findings. A single review may take weeks and multiple visits to the developer facility to resolve all the compliance issues.

The purposes of the applicant review are to:

- Ensure the process is compliant and
- Ensure the product is satisfactory.

While reviewing for compliance, the applicant may identify problems with the design. Hopefully, the developer will have already discovered most of these problems; however, some new problems may be discovered during the review process. All problems should be considered from a programmatic point of view for how they will affect the final product. They should also be considered from a process point of view (i.e., was the identified problem a one-time occurrence, or is it evidence of a systemic problem?). Consider whether a problem exemplifies a type of error that the process does not detect. If it appears to be systemic, then the process problem should be corrected.

A finding of non-compliance is when evidence shows that the developer:

1) Is not following RTCA DO-278A,
2) Is not following their plans and standards, and/or
3) Has a systemic problem with their process.

The first two examples above require evidence that the non-compliance is occurring and a reference to the requirement not being satisfied. The third example indicates there has been a finding of something that acts against the purpose of development assurance, which is to layer mitigations that prevent errors from getting into the design.

Often, the reviewer will find items that are undesirable but either have not manifested direct evidence of a problem or only loosely connect to the RTCA DO-278A guidance. These types of findings do not indicate non-compliance, but they should be noted as observations when they surface. Observations are tracked to increase visibility so that if there is ever evidence of a problem, these noted observations can become findings to be addressed.

6.5 Level of Approval Authority Involvement

The level of approval authority involvement in a software project must be determined and documented in the PSP as early as possible in the project lifecycle. The type and number of software reviews will depend on the software AL of the project, the amount and quality of RTCA DO-278A SME support, the experience and history of the applicant and/or software developer, and the service difficulty history. At a minimum, determinations on the appropriate level of approval authority involvement must include:

1) When the approval authority should be involved: the time during the software lifecycle at which an assessment can be made to determine whether the project is progressing

toward approved plans and procedures (e.g., planning, development, integration/verification, or final software approval).

2) The extent of approval authority involvement: how much and how often the approval authority is involved in the project (e.g., how many on-site reviews are conducted; how much oversight is delegated to the RTCA DO-278A SME; and how much and what types of applicant data are reviewed, submitted, recommended for approval, and approved).

3) The appropriate areas for approval authority involvement: the parts of the software processes where the approval authority should focus involvement to ensure satisfaction of the appropriate RTCA DO-278A objectives (e.g., focus on plans, design, or code).

The following items may influence the level of the approval authority involvement in the software review process:

- The AL, as determined by a system safety assessment;
- The product attributes (e.g., size, complexity, system functionality or novelty, and software design);
- The use of new technologies or unusual design features;
- Proposals for novel software methods or lifecycle models;
- The applicant's knowledge of and previous compliance with the objectives of RTCA DO-278A and, as applicable, RTCA DO-330, RTCA DO-331, RTCA DO-332, and RTCA DO-333;
- The availability, experience, and authorization of software SMEs;
- The existence of issues in the project that are associated with Section 12 of RTCA DO-278A; and
- The distribution of issue papers for software-specific aspects of the approval project.

6.6 Preparing, Conducting, and Documenting the Software Review

6.6.1 Prepare for the Review

The approval authority responsible for software approval must coordinate with the applicant to assemble the review team. The review team should include at least one person knowledgeable in software engineering, CM, and SQA and one person familiar with the system safety assessment and system requirements. Due to the PO/developer relationship, the team should consist of applicant and contractor complements for CM and quality assurance purposes.

The applicant must coordinate with the approval authority and the developer to propose an agenda for the upcoming software review at least six weeks in advance. To optimize the efficiency of the review team while on-site, the approval authority should request that software plans identified in RTCA DO-278A, Section 4.3, be available at least 10 working days prior to the review. Each team member should review the plans before arriving at the developer's facility. The approval authority should prepare a short initial briefing to introduce the team members, restate the purpose of the review, and provide an overview of the agenda. The applicant or developer should prepare a short briefing on the system under review; the software lifecycle model, processes, and tools used; and any additional considerations made.

6.6.2 Notify the Applicant

At least six weeks prior to the review, the approval authority must notify the applicant in writing about the approver's expectations in the software review. The following information should be included in the notification letter:

- The purpose of the review;
- The type of review (e.g., planning, development, verification, final, or other);
- The date and duration of the review;
- A list of review participants with contact information;
- A request that the software plans identified in RTCA DO-278A, Section 4.3, be provided;
- A request that pertinent lifecycle data be made available at the time of review;
- An indication of which RTCA DO-278A objectives will be assessed;
- A suggestion that applicants conduct their own self-assessments before the review; and
- A request that the responsible managers; developers; and CM, verification, and quality assurance personnel be available to answer questions.

6.6.3 Conduct the Review

A typical review includes the following elements:

- **An approval authority entry briefing,** including (1) an introduction of review team members, (2) a restatement of the purpose of the review, and (3) an overview of the review agenda.
- **An applicant briefing**, including (1) the system under review; (2) the software lifecycle model, processes, and tools used; and (3) any additional considerations.
- **A software developer's briefing**, including:

  1) Availability of facilities;
  2) The availability of lifecycle data;
  3) Any personnel schedule constraints;
  4) An overview of the system;
  5) Descriptions of the interaction of the system with other systems, the system architecture, the software architecture, and the software lifecycle model (including tools and methods);
  6) Progress against previous action items or issue papers (if appropriate);
  7) The current status of the development (including status accounting report or similar data);
  8) A summary of self-assessment results (if performed); and
  9) Any additional considerations (per RTCA DO-278A, Section 12).

- **An approval authority's review** of the applicant/developer's processes and product.

  Note: Desk reviews may be performed instead of or in addition to in-person reviews.

The preparation, performance, and reporting of desk reviews will be similar to in-person reviews.

7 Document the Review

Documentation of the review is completed in the following steps:

1) **Record the Review Results:** The review results must be recorded and should, at a minimum, include the following:

   - A list of each lifecycle data item reviewed, including document name, control identity, version, date, requirement identification (where applicable), source code module (where applicable), paragraph number (where applicable), and review results.
   - A description of the approach taken to identify findings or make observations.
   - An explanation of the findings or observations as related to the unsatisfied objectives of RTCA DO-278A, documented with detailed notes. Each objective requires a summary of what was done and a discussion as to why the objective was not satisfied. When necessary, examples should be included to ensure that the approach and findings can be understood and reconstructed at some future date, if needed.
   - Any necessary actions for the applicant or the approver.
   - A list of all current or potential issue papers.

2) **Deliver an Exit Briefing:** The final briefing to the applicant and/or developer must concisely and accurately summarize the review findings and observations. Findings and observations should be presented with specific reference to RTCA DO-278A objectives, approval basis, policy, guidance, or other approval documentation. The applicant and/or developer should be given the opportunity to respond to the findings and observations. The applicant and/or developer response may not be immediate (i.e., it may be several days later), since it typically takes some time to process the review findings and observations.

3) **Prepare a Review Report:** Following the review, the approval authority must summarize all review findings, observations, and required actions in a report. The report should be coordinated with and sent to the applicant within 10 working days of the review.

4) **Identify and Prepare Issue Papers (as needed):** Issue papers are a means of documenting technical and approval issues that must be resolved before approval. They provide the necessary communication between the applicant and approval authorities. Issue papers should be identified, prepared, and resolved as soon as possible after the issue is discovered. Issue papers prepared for software-specific issues should be coordinated with Safety and Technical Training.

8 Approving Reused Software Lifecycle Data

This section provides guidelines for determining whether software lifecycle data produced and approved for one approval project can be approved for a follow-on project. Approval for reuse could minimize the repetition of work while maintaining an equivalent level of development assurance.

8.1 Software Suitable for Reuse

If properly planned and packaged, software lifecycle data may be reused from one project to

the next with minimal repetition of work. For example, the software plans, requirements, design, and other software lifecycle data (as documented in an SCI) for an Airport Surveillance Radar (ASR) may have been originally approved for the ASR-9 but could possibly be reused for ASR-11. Sample items suitable for reuse include:

- **Software Plans and Standards:** These include software undergoing non-substantive changes, such as:
  - A change to the program name or
  - Configuration changes made for reasons other than design changes (e.g., document format changes, drawing modifications, or documentation system changes).
- **TQ Data:** The approval authority can approve this item for reuse if the tool is used in the qualification approval exactly as it was used in part of the original approval and the applicant has access to the TQ data. This is true even if some of the features were qualified but not used during the original approval. The applicant should ensure that the same version of the tool is being used as that which was supported by the qualification data. The approval authority will not approve reuse if the applicant uses an additional or different tool functionality than what was previously qualified.
- **Software Compiler Libraries:** The approval authority can approve reuse of library sets in the original approval project if the new project uses the same library functions in the same way.
- **Software Requirements, Design, Code, Verification Procedures, and Verification Results:** The approval authority may approve these items for reuse after the applicant makes a thorough change impact analysis. This analysis is to confirm that the requirements, design, code, procedures, and results are unaffected by and unchanged from the previous approval effort.
- **Configuration Items:** These may be approved for reuse in their entirety if the approval authority and SMEs determine that the items meet the considerations and guidelines established in this appendix and the configuration of the software lifecycle data has not been changed. Configuration item requirements verified at a higher level (i.e., system level) should be identified in the original configuration and verified again before reuse.
- **Additional Considerations:** Projects not using RTCA DO-278A may have additional considerations not documented in this section. Approval authorities must evaluate them on a case-by-case basis. The applicant should contact the approval authority for guidance.
- **Safety Considerations:** If the approval authority finds software lifecycle data acceptable for reuse, no further design approval is required. Table L.4 illustrates the considerations that govern whether the approval authority will approve software reuse.

Uncontrolled copy when downloaded

Table L.4: Reuse Approval Considerations

Approval authority may approve software lifecycle data for reuse if the reuse:	• Has no adverse effect on the original system safety margins and • Has no adverse effect on the original operational capability unless accompanied by a justifiable increase in safety.
Approval authority will not approve software lifecycle data for reuse if the reuse:	• Adversely affects safety, • Exceeds a pre-approved range of data or parameters, or • Exceeds an equipment performance characteristic.

8.2 Factors Affecting Reuse

The following sections discuss factors that affect the ability to reuse software lifecycle data.

8.2.1 Unchanged and Applicable Software Lifecycle Data

Any of the software lifecycle data in RTCA DO-278A, Section 11, is suitable for reuse. To meet the requirements in Section 8.3 of this appendix, the software lifecycle data should be unchanged and should apply to the project for which reuse is being considered.

8.2.2 In-Service Problems

In-service problems with previous applications can limit reuse. The applicant needs to analyze all developers' open problem reports to ensure that the reusable portion of the new software is not affected. If the reusable portion of the new software is affected, changes to correct that software lifecycle data should be made or the software should not be used.

8.2.3 Operational Environment and Software Development Environment

Applicants must determine whether the software data apply to the subsequent project's development by assessing the similarity of both the operational environment and the software development environment. Applicants should:

1) Assess the operational environment by evaluating the end-to-end performance requirements and the Operational Safety Assessment;
2) Refer to the Software Lifecycle Environment Configuration Index in RTCA DO-278A, Section 11.16, when assessing the software development environment;
3) Demonstrate that operational and software development environments are the same or that the environments produce results identical to those that were previously approved; and
4) Assess any outstanding problem reports.

8.3 Reuse Approval Guidelines

The approval authority must ensure that the applicant has met the following guidelines before granting approval for reused software lifecycle data:

1) The software lifecycle data have not changed since the previous approval;

Uncontrolled copy when downloaded

2) The AL of each software application is equal to (or more stringent than) the AL of the original approval effort;
3) The range and data type of inputs to the configuration item are equivalent to its approved predecessor;
4) The configuration item is embedded on the same target computer and is used the same way operationally as in the original approval project;
5) Equivalent software/hardware integration testing and system testing have been conducted on the same target computer and system as in the original approval project;
6) The applicant has followed the safety considerations and considered the reuse factors outlined in this section; and
7) The software lifecycle data and the rationale for reuse of each item have been documented in the “Additional Considerations” portion of the PSAA. The applicant’s PSAA should include method of use, integration, and documentation for the reused configuration item. The PSAA should be submitted as early as possible in the development program and should also document all references to the previously approved project and the project number, as applicable.

The approval authority responsible for the subsequent approval must review the PSAA and notify the applicant as to whether the proposal is acceptable. The approval authority will provide rationale supporting the decision.

Uncontrolled copy when downloaded

Appendix M

Overview of RTCA DO-278A and Its Required Deliverables

Overview of RTCA DO-278A and Its Required Deliverables

1 Purpose

This appendix provides an overview of RTCA[1] DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*; the deliverables it describes must be approved by the government.[2]

2 Applicable Policy and Related Documents

This appendix does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the Air Traffic Organization (ATO) Safety Management System (SMS), which provides guidance on fulfilling requirements set forth in the current version of FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. This appendix also supplements FAA Acquisition Management System (AMS) policy.

The primary reference materials in this guidance are the current editions of the following:

- Safety Risk Management Guidance for System Acquisitions (SRMGSA);
- AMS, Section 4.12, *National Airspace System Safety Management System*;
- ATO SMS Manual; and
- FAA Order JO 1000.37.

3 Overview

3.1 RTCA DO-278A

RTCA DO-278A is the standard agreed upon by the industry and government for assuring that the software produced during system development is appropriate for a given level of safety. RTCA DO-278A was created because of the need for developmental assurance. It is specific enough to outline objectives that must be met, but vague enough to allow for flexibility in meeting them. RTCA DO-278A provides Verification and Validation (V&V) guidance to ensure a designated level of safety by eliminating classes of error that occur in software design.

Development assurance is an organized, rigorous approach to error prevention. It consists of lifecycle processes (requirements, design, integration, and approval) and concurrent integral processes (planning, development V&V, quality assurance, Configuration Management (CM), and approval coordination) that exist throughout the life of the project.

RTCA DO-278A is not designed to stipulate the exact contents of each process. However, it does define measurements of quality, some of the necessary relationships among the processes, and the mandatory outputs of each process. The outputs include the items listed below.

- Plan for Software Aspects of Approval (PSAA)
- Software Development Plan (SDP)
- Software Verification Plan (SVP)

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

2. An RTCA user identity and password are required to download RTCA documents. Federal Aviation Administration employees may obtain an RTCA membership by contacting RTCA.

- Software Configuration Management Plan (SCMP)
- Software Quality Assurance Plan (SQAP)
- Tool Qualification Plan
- Tool operational requirements
- Software requirements standards
- Software design standards
- Software coding standards
- Software requirements data
- Trace data
- Design description
- Software verification results
- Software verification cases and test procedures
- Source code
- Executable Object Code (EOC)
- Adaptation Data Item file
- Problem Reports (PRs)
- Software quality assurance records
- Software CM records
- Software Environment Configuration Index (SECI)
- Software Configuration Index (SCI)
- Software Accomplishment Summary (SAS)

RTCA DO-278A does not attempt to predict possible business arrangements. As such, it only discusses two primary parties: the system developer and the approval authority. It specifically excludes matters concerning the structure of the system developer's organization, the developer's commercial relationships with their suppliers, and any personnel qualification criteria. Furthermore, RTCA DO-278A places the burden of supplier oversight on the system developer and not the approval authority.

In practice, the Program Office (PO) does not typically develop software. Instead, the work is contracted to a commercial system developer (and occasionally another FAA office). To ensure a comprehensive safety program is conducted, the PO must develop a Program Safety Plan (PSP) per guidelines in SRMGSA Appendix A. The PSP describes how the PO intends to provide the oversight to ensure the system developer will meet RTCA DO-278A requirements and generate a PSAA and all other required documents. The PSP must also detail how the Program Management Organization (AJM) will play an early role in reviewing documentation prior to final approval. The system developer's System Safety Program Plan must be consistent with the safety program outlined in the PSP.

For detailed assistance on appropriate content for the PSP, see Appendix A. The process is outlined in the following steps:

1) The system developer produces the software in compliance with RTCA DO-278A.
2) The system developer's Software Quality Assurance (SQA) personnel verifies compliance to RTCA DO-278A.
3) The PO verifies that the developer's SQA activities comply with RTCA DO-278A.

4) The approval authority verifies the PO's activities.
5) The approval authority approves RTCA DO-278A compliance and related artifacts.

As such, all documentation that is submitted to the approval authority must be reviewed for compliance by the PO and SQA.

RTCA DO-278A requires that the system developer submit—at a minimum—the PSAA, SCI, and SAS to the approval authority. These three documents summarize the entire project at its beginning and at its end. The SRMGSA requires the PO to evaluate all lifecycle data and provide evidence of compliance to the ATO Chief Safety Engineer. The PO must approve the system developer's submittals per the requirements of the Statement of Work (SOW) and other contractual language. AJM is the product approval authority, and the ATO Chief Safety Engineer is the safety approval authority.

Due to their importance, the following sections elaborate on the contents of the PSAA, the SCI, and the SAS. However, these elements only make up the basic outline of the documents. RTCA DO-278A provides more detail on the contents of the individual sections. The PSAA discusses how the SDP, SVP, SCMP, and SQAP are going to account for and check all required activities. The SCI describes the product itself. The SAS highlights what has been accomplished to verify that all planned activities have been completed. The philosophy behind these documents is that all activities should be planned for and reviewed.

3.2 PSAA

The PSAA demonstrates how the program will comply with AMS, Section 4.12, which requires the developer to have a development assurance program that meets the requirements of the latest version of RTCA DO-278A or an equivalent standard. The PSAA serves as the primary means for communicating the proposed development methods to the approval authority. Per AMS, Section 4.12, software-intensive systems can establish a development assurance program in accordance with RTCA DO-278A; this is an acceptable way to demonstrate that a software product was developed at the appropriate level of rigor. The approval authority uses the required output to determine whether the system developer is proposing a software lifecycle that is commensurate with the level of rigor required for the software being developed.

The PSAA provides a summary of the SDP, the SVP, the SCMP, and the SQAP by describing the overall project and how developmental assurance objectives will be satisfied. If the system developer subcontracts work to another supplier, the PSAA must also cover how the system developer will perform supplier oversight.

The SRMGSA requires that the system developer submit the PSAA for FAA approval. AJM has been designated the approval authority. It is critical that the system developer submit the PSAA to the government in a timely manner so meaningful input can be provided. This will allow the PSAA to be approved and implemented prior to the critical design review. Ideally, the PSAA should be incorporated into the system developer's overall development plan and should be approved prior to the closeout of the System Specification Review conducted by the system developer.

When using RTCA DO-278A as a means of ensuring compliance with AMS, Section 4.12, the associated RTCA DO-278A supplements must also be used where applicable. The following

documents address certain software development techniques and can add, delete, or modify objectives, activities, and lifecycle data in RTCA DO-278A:

- RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A*;
- RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*; and
- RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*.

Guidance within a particular supplement must be applied when using the addressed technique. The PSAA must identify applicable supplements and describe the intended use of each. If a supporting supplement is not being used, the PSAA must identify why a supplement (such as Formal Methods) is not being used in the verification activities of software development.

An effective PSAA clearly details the following elements:

- **System Overview:** For the current system and any proposed changes, describe functions, allocation to hardware/software architecture, processor(s), hardware/software interfaces, and safety features.
- **Software Overview:** For the current software and any proposed changes, describe software functions, partitioning, redundancy, resource sharing, fault tolerance, timing, and scheduling.
- **Software Lifecycle:** Summarize each lifecycle (requirements, design, code, verification, SQA, and software CM) and how the objective of each software lifecycle is satisfied by organizational structure and responsibilities.
- **Software Lifecycle Data:** Discuss how data are produced and controlled, the relationship between data, the data to be submitted and in what form it will be submitted, and the means of submittal.
- **Schedule:** Describe how visibility is provided to the approval authority to allow for planning.
- **Supplier Oversight:** Describe how the applicant will have visibility into their suppliers' and sub-tier suppliers' activities. This includes the activities of suppliers and vendors of Commercial Off-the-Shelf (COTS) software components.
- **Additional Considerations:** Describe the basis of approval, means of compliance, level of assurance, software contribution to failures, previously approved software, and COTS software. For development tool qualification, reference the Tool Qualification Plan. If no Tool Qualification Plan has been developed, include the pertinent information in the PSAA. If applicable, include a justification as to why the tool does not require qualification.
- **Approval Considerations:** This may include alternative means of compliance.
- **Attachments:** These could include, but not be limited to:
    - RTCA DO-278A Compliance Gap Analysis Evaluation Worksheet (see Appendix K).
    - Software lifecycle data.

The FAA usually requires that the contractor submit the PSAA as a deliverable for 90 days after the start of the contract. In some situations, the FAA may require that a preliminary PSAA be submitted with the proposal to ensure that the contractor has planned and budgeted for an adequate PSAA. Since the system safety effort can suffer if the procurement is cost-competitive, an approval requirement for the PSAA provides the FAA the necessary control to minimize this possibility.

Changes to an approved plan must be coordinated with the approval authority to ensure compliance. Plans are more than a documentation requirement; they must be followed, or the project cannot be approved.

3.3 SCI

The primary purpose of an SCI is to be a software parts list for a specific software release and/or build. It functions as a master list for the configuration of the software items under configuration control. The SCI must contain or reference the SECI. The SECI identifies the configuration of the software lifecycle environment. This index is written to aid reproduction of the hardware and software lifecycle environment and software regeneration, reverification, or modification.

For each software release, an SCI must be developed to document the software configuration, build instructions, and load/verification procedures. The SCI must include:

- The software product;
- Each Source Code component;
- EOC and Adaptation Data Item files;
- Previously developed software in the software product;
- Software lifecycle data;
- Archive and release media;
- Instructions for building the EOC and Adaptation Data Item files;
- Data integrity checks in EOC, if used;
- Procedures, methods, and tools for modifying the user-modifiable software;
- Procedures and methods for loading the software into the target hardware;
- Procedures used to recover the software for regeneration, testing, or modification; and
- The SECI or, if packaged separately, a reference to it. The SECI should identify:
    - The software lifecycle environment hardware and its operating system software;
    - The software development tools, such as compilers, linkage editors and loaders, and data integrity tools;
    - The test environment used to verify the software product (for example, the software verification tools); and
    - Qualified tools and their associated tool qualification data.

There may be multiple iterations of the SCI submitted for approval as the system design matures. The SCI should be updated as necessary with each version update of the product and before every formal run of the software test suite. The SRMGSA requires that the system developer submit the final SCI for FAA approval. AJM is the designated approval authority.

3.4 SAS

As required by the SRMGSA, the SAS is the primary data item for showing compliance with the PSAA. The SAS must be signed by the FAA approval authority (i.e., by AJM) prior to system

operation. This means that prior to submitting the document for approval, the system developer and the government must coordinate and conduct a document review.

The plan for compliance to software assurance regulations (RTCA DO-278A) is contained in the PSAA. Once the PSAA is approved, the project has direction to proceed. In the course of development, a change in direction may be warranted that results in a deviation from the approved plans. The system developer must schedule a meeting with the approval authority to brief the changes. If the approval authority agrees that the changes are compliant, the system development may proceed. Deviation from the PSAA may need to occur a few times during development, but if the approval authority agrees that the deviation is sufficiently documented, the PSAA does not need to be rereleased each time.

At the end of the project, the system developer must produce an SAS that documents all the deviations from the original PSAA, especially those that were not previously agreed upon. The content only needs to provide sufficient information to identify the new methods and the original processes that were changed. This documents the prior agreements and provides a vehicle to approve any methods/processes not already coordinated.

The SAS must provide the final characteristics about the software and list PRs that were generated and processed through the Change Review Board. A PR can be resolved for the following reasons:

- The PR should never have been generated.
- The PR pertained to a function that was not implemented in the final design.
- The PR was evaluated, fixed, verified, and closed.
- The PR could not be fixed in time for deployment and is still open.

The open PRs must be evaluated, and instructions must be established for how to address these PRs until fixes for them are implemented.

The SAS must include a traceability matrix showing (1) how each RTCA DO-278A objective was met and (2) the SQA records with evidence of compliance for each objective. The approval authority must be able to validate that there is sufficient evidence showing that a project complies with RTCA DO-278A.

The SAS must cover the following topics:

- **System Overview:** Provide an overview of the system, including a description of its functions and their allocation to hardware and software. Also include a description of the system's architecture, the processor(s) it uses, its hardware/software interfaces, and its safety features. This section must also describe any differences from the system overview in the PSAA.
- **Software Overview:** Briefly describe the software functions with emphasis on the safety and partitioning concepts used, such as resource sharing, redundancy, multiple-version dissimilar software, fault tolerance, timing, and scheduling strategies. It must explain differences from the software overview proposed in the PSAA.
- **Approval Considerations:** Restate the approval considerations described in the PSAA and describe any differences from the original plan.

- **Software Lifecycle:** Summarize how the software lifecycle has unfolded, and explain the differences between the actual software lifecycle and the software lifecycle processes originally proposed in the PSAA.
- **Software Lifecycle Data:** Describe any differences between the collected software lifecycle data and the lifecycle data proposed for collection in the PSAA. Also describe the relationship between lifecycle datasets as well as their relationships to other data defining the system; and describe how the data were made available to the approval authority. This section explicitly references, with configuration and version identifiers, the applicable SCI and SECI. Detailed information regarding configuration identifiers and specific versions of software lifecycle data are provided in the SCI.
- **Additional Considerations:** Summarize any specific considerations that may warrant the attention of the approval authority. Explain any differences from the proposals contained in the PSAA regarding such considerations. References should be made to data items applicable to these matters, such as contractual agreements or special conditions.
- **Supplier Oversight:** Describe how supplier processes and outputs comply with system plans and standards.
- **Software Identification:** Identify the software configuration by part number and version.
- **Software Characteristics:** State the EOC size, timing margins (including worst-case execution time), memory margins, resource limitations, and the means used for measuring each characteristic.
- **Change History:** If applicable, include a summary of software changes with attention to changes made due to failures affecting safety, and identify any changes in / improvements to the software lifecycle processes since the previous approval.
- **Software Status:** Summarize any PRs unresolved at the time of approval. The PR summary includes a description of each unresolved problem and any associated errors, functional limitations, operational restrictions, potential adverse effects on safety, justification for allowing the PR to remain open, and details of any mitigating action that has been or needs to be taken.
- **Compliance Statement:** Include a statement of compliance and a summary of the methods used to demonstrate compliance with criteria specified in the software plans. Address additional rulings made by the approval authority and any deviations from the software plans, standards, and the PSAA not covered elsewhere in the SAS.

The results of the SAS must be summarized in the System Safety Assessment Report.

4 Establishing the Contractual Requirement

The PO must establish the contractual requirements in the SOW to ensure that they have access to all the lifecycle data as well as a schedule to ensure the necessary documents are delivered in a timely manner. The SOW should also account for the review of the documents by all the approval organizations and consider that multiple revisions may be required before a document can be finally approved. RTCA DO-278A requires that all documentation be correct. Changes to the project may require updates to all impacted documents. The Data Item Descriptions (DIDs) for a PSAA, SCI, and SAS are available in the DID Library. The PO may tailor the DIDs as necessary.

Appendix N
Acronyms

Acronyms

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

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

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