FAA
Air Traffic Organization

Air Traffic Organization
Safety Management System Manual

Version 2.1
May 2008

SMS Resources

Each Service Unit has a designated Safety Manager and Safety Engineer(s) who can provide additional guidance regarding the Air Traffic Organization (ATO) Safety Management System (SMS).

As with any other SMS component or topic in this manual, Safety Services is also available to provide additional guidance and/or information via email at 9-AWA-ATO-SRM-Safety-Service@faa.gov.

Table of Contents

Foreword ..... **i**

Chapter 1 – Safety Management System (SMS) Overview **1**

1.1 Introduction 1
1.2 Purpose 4
1.3 Scope 5

Chapter 2 – Safety Policy **6**

2.1 Introduction 6
2.2 Requirements 6
2.3 Roles and Responsibilities 7
2.4 Safety Oversight 10

Chapter 3 – Safety Risk Management **13**

3.1 Introduction 13
3.2 SRM Overview 13
3.3 Applicability of SRM 18
3.4 Planning 20
3.5 Preliminary Safety Analysis 23
3.6 When Further Safety Analysis Is Required 25
3.7 Phase 1: Describe System 27
3.8 Phase 2: Identify Hazards 31
3.9 Phase 3: Analyze Risk 37
3.10 Phase 4: Assess Risk 43
3.11 Phase 5: Treat Risk 45
3.12 SRMD 51
3.13 SRMD Approvals 55
3.14 Accepting Risk 57
3.15 Tracking Changes 59

Chapter 4 – Safety Assurance **61**

4.1 Introduction 61
4.2 Audits and Evaluations Overview 61
4.3 Air Traffic Evaluations and Auditing Program 63
4.4 NASTEP 65
4.5 IOT&E 65
4.6 SMS Evaluations and Audits 66
4.7 Safety Data Tracking and Analysis 68

Chapter 5 – Safety Promotion **77**

5.1 Introduction 77
5.2 Safety Culture 77
5.3 SMS Training 80

Appendices

Appendix A – Glossary of Terms……..A-1
Appendix B – Acronyms/Abbreviations……B-1
Appendix C – ATO Safety Guidance Process……C-1
Appendix D– References to FAA Documents Related to SMS Requirements……D-1
Appendix E – SRMDM Template…….. E-1
Appendix F – SRMDM Review Checklist……F-1
Appendix G – Hazard Identification and Analysis Tools and Techniques……G-1
Appendix H – Documenting Existing Hazards Process……H-1
Appendix I – Bow-Tie Model Example……..I-1
Appendix J – High-level SRMD Guidance…… J-1
Appendix K – SRMD Template……K-1
Appendix L – SRMD Review Checklist…….. L-1
Appendix M – SRM and Operational Changes to the ATC System…… M-1
Appendix N – Deployment Planning Process with SRM…… N-1

List of Tables

Table 3.1: Selection of Hazard Identification and Analysis Tools and Techniques.....35
Table 3.2: Examples of Existing Controls 38
Table 3.3: Severity Definitions 39
Table 3.4: Likelihood Definitions 42
Table 3.5: Safety Order of Precedence 49
Table 3.6: Sample Recommended Control Implementation/Monitoring Plan 51
Table 3.7: SRMD Approval Level Requirements 55
Table 3.8: Risk Acceptance Summary.....58
Table 3.9: Example of a NAS Change Tracking Matrix 59
Table 4.1: Safety Data Reporting Documents and Processes.....74

List of Figures

Figure 1.1: The Lesson of Heinrich's Triangle 2
Figure 1.2: SMS Integration Diagram 3
Figure 2.1: Safety Directors, Safety Managers, and Safety Engineers.....10
Figure 2.2: AOV/ATO Relationship 12
Figure 3.1: Defenses in Depth Philosophy.....15
Figure 3.2: SRM and the NAS 19
Figure 3.3: SRM Decision Process 23
Figure 3.4: Spectrum of NAS Change Examples.....24
Figure 3.5: SRM Safety Analysis Phases 26
Figure 3.6: How to Accomplish a Safety Analysis.....27
Figure 3.7: 5M Model 29
Figure 3.8: The Bow-Tie Model.....34
Figure 3.9: Risk Matrix 44
Figure 3.10: SRMD Naming Convention.....54
Figure 4.1: SRMD, IOT&E Documentation, and Process Links 66
Figure 4.2: Incident Reporting.....71

Foreword

ATO's most fundamental imperative is to ensure the safety of the national airspace system. Thanks to our 34,000 employees, we run the safest, most efficient system in the world. Safety can be effectively determined not only by the current absence of accidents, but also the presence of safe conditions well into the future.

Therefore, as we build the Next Generation Air Transportation System, the resulting cross-organizational changes to the NAS will require us to maintain an intensive, proactive, and systematic focus on safety. This focus is achieved through the implementation of the Safety Management System (SMS).

The SMS formally integrates the ATO's safety-related operational processes, procedures, policies, and programs. SMS stresses safety assurance, through the analysis of safety data, and promotes a vibrant safety culture among our workforce. SMS also guarantees that every step we take toward NextGen, we are identifying, analyzing, and mitigating risk.

This manual outlines the procedures and responsibilities regarding the functioning of the SMS. While the manual focuses on clarifying safety management processes of the organizations within the ATO, this manual is applicable to all FAA organizations that promote and approve changes that affect the provision of air traffic control and navigation services.

This manual was developed as the result of a consolidated, agency-wide effort and reflects current international best practices. Safety experts and managers from across the FAA contributed to its development. This version of the manual marks an important next step toward a complete and integrated SMS in the FAA.

Hank Krakowski
Chief Operating Officer
Air Traffic Organization

Chapter 1 – Safety Management System (SMS) Overview

1.1 Introduction

1.1.1 Purpose and Structure of the SMS Manual

In support of the effort to provide a safer National Airspace System (NAS) using the Safety Management System (SMS), this manual describes the Air Traffic Safety Oversight Service (AOV) safety requirements and responds to International Civil Aviation Organization (ICAO) safety process requirements for the Air Traffic Organization (ATO). The manual also provides guidance, processes, and tools to ATO personnel for managing the safety of the NAS, building on existing ATO safety management capabilities. This manual was created to provide specific operational process information to support the daily activities of ATO employees. It describes the functions, components, and principles of the SMS and provides the guidance to apply them effectively. ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*, requires the use of the current version of the ATO SMS Manual and the safety standards defined in it.

The first chapter of this manual is an introduction to the SMS. The remaining chapters are organized by the four components of the SMS: safety policy, Safety Risk Management (SRM), safety assurance, and safety promotion. Each chapter is described below.

a. **Chapter 1 – SMS Overview:** An SMS introduction that includes the definition of the SMS, how it originated in the ATO, and the objectives, scope, and products.
b. **Chapter 2 – Safety Policy:** A description of the safety management requirements, which are consistent with AOV SMS and ICAO safety process requirements; roles and responsibilities related to the SMS and the relationships among the different roles; why safety oversight is necessary; and responsibilities and authorities of AOV.
c. **Chapter 3 – Safety Risk Management:** The types of changes evaluated for safety risk; processes and guidance available for determining the level of safety analysis required; detail and documentation required for safety analysis; SRM process; SRM terminology, tools, and techniques; risk acceptance requirements; tracking required NAS changes; and the development and approval of SRM documentation (including roles involved in both activities).
d. **Chapter 4 – Safety Assurance:** The importance of safety reviews and evaluations in the SMS; assurance programs, including the Air Traffic Evaluation and Auditing Program, the NAS Technical Evaluation Program (NASTEP), the Independent Operational Test and Evaluation (IOT&E) process, Independent Safety Assessments, and SRM audits; importance of safety data; types of data; how data are collected and reported; processes for reporting safety incidents and accidents; relationship between incident investigations and SRM; monitoring of mitigations through safety data tracking and analysis; and existing safety data reporting documents and processes.
e. **Chapter 5 – Safety Promotion:** What a safety culture is; why it is important; responsibilities within it; and SMS training.

Appendix A, *Glossary of Terms,* contains a glossary of terms used in this manual. These terms are consistent with AOV Safety Oversight Circular (SOC) 08-06, *ATO Safety Management System (SMS) Definitions.* In addition, Appendix B, *Acronyms/Abbreviations*, contains a list of acronyms used in this document.

1.1.2 Setting the Stage: The Importance of Safety

In the context of the SMS, safety is defined as freedom from unacceptable risk. This definition derived from multiple safety definitions. As stated in the Federal Aviation Administration (FAA) Flight Plan, "Safety is our bottom line. It's non-negotiable."[1] Safety must be the principal consideration of all FAA activities.

Heinrich's Triangle is an internationally recognized model that illustrates accident causation. The adaptation of Heinrich's Triangle in Figure 1.1 graphically depicts the relationship between unsafe acts, hazardous conditions, incidents, and accidents. For every catastrophic accident, there are many incidents or minor accidents. For each incident, there are numerous hazards and many unreported unsafe acts. The model states that the most effective accident prevention programs focus on collecting, analyzing, and investigating incident data and the most effective way to prevent accidents is to focus on preventing hazardous conditions before an incident occurs. The SMS allows the ATO to focus on minimizing unsafe acts in order to improve safety. The concept of safety data sharing is covered in detail in Chapter 5, *Safety Promotion*.

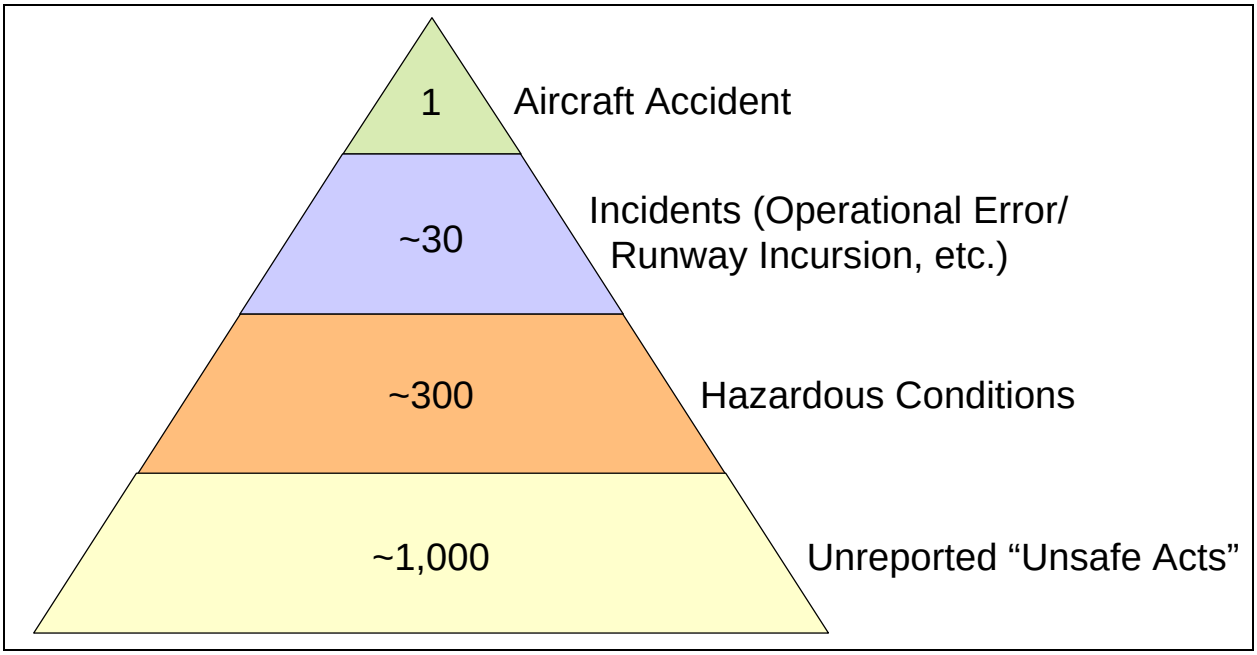


Figure 1.1: The Lesson of Heinrich's Triangle

Note: The quantities represented in Figure 1.1 are for illustrative purposes only and are not based on actual aviation data.

Safety is often equated to meeting a measurable goal, such as an accident rate that is less than an acceptable target. However, the absence of accidents does not ensure a safe system. For each hazardous condition, many unreported unsafe acts or circumstances might exist. Therefore, safety must be constantly monitored and assessed, which the SMS helps to accomplish.

[1] FAA Flight Plan 2008–2012, page 18 (available at http://www.faa.gov/about/plans_reports/).

1.1.3 SMS Introduction

The SMS provides a systematic and integrated method for managing the safety of Air Traffic Control (ATC) and navigation services in the NAS. The SMS is divided into the following four components:

a. **Safety Policy:** The SMS requirements and responsibilities for all components of the NAS owned and/or operated by the ATO, as well as safety oversight of the ATO.
b. **SRM:** The processes and practices used to assess changes to the NAS for safety risk, the documentation of those changes, and the continuous monitoring of the effectiveness of any controls used to reduce risk to acceptable levels.
c. **Safety Assurance:** The processes used to evaluate and ensure safety of the NAS, including evaluations, audits, and inspections, as well as data tracking and analysis.
d. **Safety Promotion:** Communication and dissemination of safety information to strengthen the safety culture and support the integration of the SMS into operations.

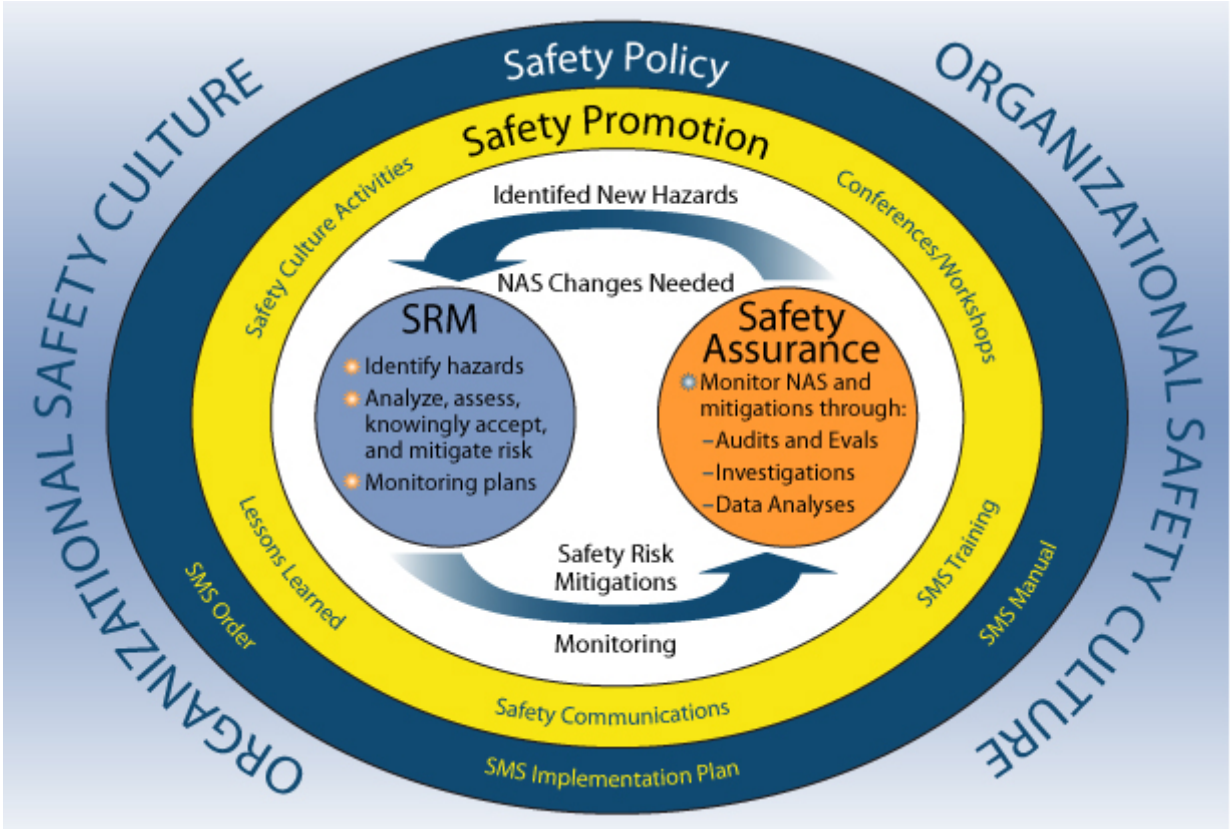


Figure 1.2: SMS Integration Diagram

Figure 1.2 depicts how the four SMS components described in this manual—safety policy, SRM, safety assurance, and safety promotion—interact with one another. Safety policy includes documents such as ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*, the SMS Implementation Plan, and this manual. The safety policy provides the framework for the SMS. It directs the ATO to perform all of the SMS activities within the other three components. At the core of the SMS are SRM and safety assurance. The outputs of these two components feed directly into one another. The ATO uses the SRM process to develop safety risk mitigations. Through safety assurance, the ATO monitors those mitigations

and identifies new hazards or necessary NAS changes, which must be analyzed for safety risk using the SRM process. Just as policy provides the framework for the SMS, safety promotion encompasses all of the SMS activities. Safety promotion allows the ATO to share successes and lessons learned. It also provides a means for ATO employees to understand the importance of safety as well as their impact on it.

1.2 Purpose

1.2.1 SMS Purpose

The overall goal of the SMS is to provide a safer NAS. The SMS provides a common framework to assess safety risks associated with changes to the NAS. It addresses all aspects of ATC and navigation services, including (but not limited to) airspace changes, air traffic procedures and standards, airport procedures and standards, new and modified equipment (hardware and software), and associated human interactions. The SMS facilitates cross-functional SRM among ATC service providers and ensures intra-agency stakeholder participation in solving the safety challenges of an increasingly complex NAS. The SMS helps reduce the number of isolated safety decisions, thus contributing to the more efficient use of time and resources. In addition, the SMS includes processes to collect and analyze safety data; conduct safety reviews, audits, and evaluations; investigate air traffic incidents; and continuously monitor data to ensure NAS safety.

The SMS continues to evolve as a result of lessons learned through the application of SMS tools and concepts, changing technologies, advances in aviation operations, and improved techniques for managing risk. In the “end state,” the SMS will be an integrated collection of processes, procedures, policies, and programs used to assess, define, and manage the safety risk in the provision of ATC and navigation services. It will provide a formalized, closed-loop, proactive approach to system safety.

1.2.2 Background of ATO SMS Implementation

Aviation safety is the fundamental mission of the FAA. The Federal Aviation Act of 1958 created the Agency and charged it with establishing and operating the United States’ ATC system to control and maintain a safe NAS.

In 2000, the FAA Administrator directed an FAA team to study the concept of an SMS. Shortly thereafter, management concluded that the design, development, and implementation of an SMS were important next steps for aviation safety.

In addition, in November 2001, ICAO amended Annex 11 to the Convention, *Air Traffic Services*,[2] to require that member states establish an SMS for providing ATC and navigation services. The SMS requirements described in Annex 11 are further detailed in ICAO Document 4444, *Procedures for Air Navigation Services, Air Traffic Management.*[3] FAA Order 1100.161, *Air Traffic Safety Oversight*, states that AOV is responsible for establishing requirements for the ATO SMS in accordance with ICAO Annex 11. In March 2007, the ATO adopted ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*, which establishes the policy, roles, responsibilities, and requirements for the ATO SMS. In November 2007, the *FAA ATO SMS Implementation Plan For Fiscal Years 2008 - 2010, Version 1.0* was finalized. This plan

[2] ICAO Annex 11 to the Convention on International Civil Aviation, Air Traffic Services, Thirteenth Edition – July 2001, Section 2.26.
[3] ICAO Document 4444 (ATM/501), Procedures for Air Navigation Services, Air Traffic Management, Fourteenth Edition – 2001, Chapter 2.

documents the gaps between the ICAO safety requirements and FAA safety processes; it establishes a plan to close the gaps through activity lists, project plans, and milestones. In addition, this manual responds to ICAO safety process requirements; it also meets AOV and ATO SMS requirements.

The SMS objective to ensure that the FAA meets or exceeds its safety goals, thereby ensuring the safety of the flying public, is also reflected as strategic goals in current strategic, operating, and business plans. These plans include the *FAA Flight Plan*, the *ATO Business Plan*,[4] and the ATO Strategic Management Process (SMP).

1.3 Scope

1.3.1 Personnel/Organizations Affected by SMS

The SMS applies to all ATO employees, managers, and contractors who are either directly or indirectly involved in providing ATC or navigation services. Providing ATC or navigation services requires collaboration when Lines of Business (LOBs) outside the ATO, including but not limited to the FAA Offices of Aviation Safety (AVS) and Airports (ARP), affect the safety of the NAS. Chapter 2, *Safety Policy,* further describes this collaboration. In most cases, this will equate to ARP and/or AVS following the SRM process when proposing changes to the NAS.

1.3.2 SMS Scope

The SMS provides clear processes and methods to identify and address those safety hazards that originate within the NAS or in which some element of the NAS is a contributing factor. For example, while the SMS does not directly address the causes of an in-flight emergency due to an aircraft system malfunction; the ATC procedures for handling an in-flight emergency must not contribute to the possibility of the emergency resulting in an accident or other negative impact on safety.

In addition, the SMS does not directly address occupational safety (i.e., the Occupational Safety and Health Administration (OSHA)), environmental policies, physical security, or information security because the FAA already has robust programs in those areas. Instead, the SMS focuses on the safe provision of ATC and navigation services. However, when personnel identify OSHA and/or security issues through SMS processes, they should contact the appropriate office for coordination on the issue and appropriate resolution.

1.3.3 SMS Products

The products of the SMS include safety risk assessments, safety data, and safety assurance and evaluation reports. These products document and support decision-making on proposed changes that impact safety. They also support the identification, prioritization, and implementation of safety enhancements for ATC and navigation services.

The SMS builds on, and must be integrated into, existing ATO and FAA processes and procedures (e.g., Acquisition Management System (AMS) processes, system safety engineering, test and evaluation, facility evaluation and auditing, equipment inspection, and many data collection and analysis programs/systems). In some cases, existing processes and documentation may need to be made more formal to comply with the SMS.

---

[4]The current versions of the FAA Flight Plan and ATO Business Plan can be viewed at the following web site: http://www.faa.gov/about/plans_reports/.

Chapter 2 – Safety Policy

2.1 Introduction

This chapter describes the overarching policy of the SMS within the ATO. It provides information pertaining to the ATO SMS. While specific SMS requirements and roles are detailed in various other policy documents, this chapter provides a brief overview of roles at the individual and organizational level, the relationships among them, and roles of other LOBs with regard to the ATO SMS.

2.2 Requirements

2.2.1 ICAO Policy

In November 2001, ICAO amended Annex 11 to the Convention, *Air Traffic Services*[5], to require that member states establish an SMS for providing ATC and navigation services. The SMS requirements described in Annex 11 are further detailed in ICAO Document 4444, *Procedures for Air Navigation Services, Air Traffic Management*.[6]

2.2.2 AOV Policy

FAA Order 1100.161, *Air Traffic Safety Oversight*, states that AOV is responsible for establishing requirements for the ATO SMS in accordance with ICAO Annex 11. FAA Order 8000.365, *Safety Oversight Circulars (SOC),* establishes SOCs as a method of providing guidance material to the ATO concerning SMS compliance and AOV directives. FAA Order 8000.86, *Air Traffic Safety Oversight Compliance Process*, contains the AOV compliance process, which is further described in Section 2.4.5. FAA Order 8000.90, *AOV Credentialing and Control Tower Operator Certification Programs,* sets forth how AOV issues and maintains credentials for ATO personnel who perform direct safety-related ATC services and/or certification on certifiable systems, subsystems, equipment, or services in support of the NAS.

2.2.3 ATO Policy

On March 19, 2007, the ATO Chief Operating Officer (COO) signed ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*. This policy documents the roles, responsibilities, and products that include the four basic tenets of the SMS—safety policy, SRM, safety assurance, and safety promotion. There are additional documents that support the SMS and these are referenced both within the order as well as in the appropriate chapters within this manual. In addition, Appendix C, *ATO Safety Guidance Process*, contains information related to the safety guidance process, a mechanism for disseminating new and revised SMS guidance material to the ATO. This process is detailed in draft ATO Order, *ATO Safety Guidance (ATO-SG)*.

2.2.4 Service Unit Subordinate Policy

Individual Service Units have the flexibility and control to tailor implementation to fit their needs, procedures, and policies within the construct of the SMS requirements. Therefore, service-specific policy may be further defined by other orders, Standard Operating Procedures (SOPs), and documents unique to a particular Service Unit. FAA Order JO 1000.39, *ATO En Route and Oceanic Services Safety Management System*, and FAA Order 7000.7, *ATO Terminal Services Safety Management System Program*, further define requirements for En

[5] ICAO Annex 11 to the Convention on International Civil Aviation, Air Traffic Services, Thirteenth Edition – July 2001, Section 2.26.
[6] ICAO Document 4444 (ATM/501), Procedures for Air Navigation Services, Air Traffic Management, Fourteenth Edition – 2001, Chapter 2.

Route and Oceanic Services and Terminal Services respectively. Appendix D, *References to FAA Documents Related to SMS,* provides more information on service-specific policy.

2.2.5 Other FAA Policy

In addition, many relevant activities pre-date the SMS and are detailed in numerous other FAA documents, orders, and processes. To minimize duplication of effort, this manual references those documents. In addition, Appendix D, *References to FAA Documents Related to SMS Requirements,* lists many of the related documents.

2.2.6 Other LOBs

As stated in the *FAA Flight Plan 2008-2012*, the FAA plans to implement an SMS in the ATO, AVS, and ARP by fiscal year (FY) 2010, followed by implementation in all appropriate FAA organizations by FY 2012.[7] Both AVS and ARP are developing policy toward that end.

2.3 Roles and Responsibilities

2.3.1 AOV Roles and Responsibilities

The FAA Administrator delegated authority to the Associate Administrator for Aviation Safety to oversee the safety of the ATO. FAA Order 1100.161, *Air Traffic Safety Oversight*, documents this authority; it describes the relationship between AOV and the ATO, as well as their respective roles and responsibilities regarding NAS safety. These roles are described in further detail in the remainder of this chapter.

2.3.2 ATO Roles and Responsibilities

While ATO Order JO 1000.37, *Air Traffic Organization Safety Management System,* addresses the roles of the ATO COO, Service Unit Vice Presidents, Safety Directors, Safety Managers, and Safety Engineers in detail, Sections 2.3.3 - 2.3.8 give a brief overview of these roles.

2.3.3 ATO COO

The ATO COO is responsible for the safety of the NAS and the implementation of the SMS within the ATO. The COO requires that organizations at all levels establish and maintain clear and unambiguous lines of authority and responsibility for ensuring safety. Additionally, the COO promotes the strengthening of the safety culture and requires that all relevant safety-related information be communicated and used in decision-making.

2.3.4 Safety Services Roles and Responsibilities

The Vice President of Safety Services is responsible for facilitating implementation of the SMS across the ATO, advocating a safety culture, conducting strategic planning for the SMS, and managing and updating SMS processes based on experiences and lessons learned. Safety Services will develop subsequent versions of this manual as well as additional guidance material (as required) to further strengthen and clarify the SMS. Several key components of SMS implementation include auditing SRM and assurance processes and outputs; facilitating coordination of SRM, evaluations and investigations, and controls with cross-organizational impacts; monitoring the safety of the NAS through data analysis; and tracking safety-critical issues to conclusion using a hazard tracking system. In addition, the Vice President is responsible for advising ATO leadership on safety-related issues, collaborating with other ICAO

[7] FAA Flight Plan 2008–2012, page 25, Objective 6 Performance Target available at the following web site: http://www.faa.gov/about/plans_reports/.

providers of ATC and navigation services to ensure harmonization of international SMS efforts, and acting as the primary ATO interface with AOV.

2.3.5 ATO Service Unit Roles and Responsibilities

All ATO Vice Presidents, directors, managers, and supervisors are responsible for implementing and adhering to SMS guidance and processes within their span of control, by requiring that existing orders, policies, directives, and/or guidance within their purview be consistent with the SMS and meet SMS requirements. This includes ensuring that all ATO personnel are trained in SMS. Other fundamental responsibilities include fostering a strong safety culture within their organizations; providing the resources (personnel and funding) necessary to become compliant and maintain compliance with the SMS requirements; ensuring the safety of those elements of the NAS within their purview; integrating SRM into the processes used to make changes to the NAS; and accepting residual safety risk associated with NAS changes within their purview. Service Units are responsible for requiring that all relevant safety information is communicated and used in decision-making, and providing information to the COO, Safety Services, and peer organizations as appropriate; ensuring that all NAS changes are documented and that information is provided to Safety Services when requested; and cooperating with evaluations and audits conducted by Safety Services and/or AOV.

These requirements pertain to leadership at all levels across the ATO. All ATO employees may affect the safety of the NAS. Directors, managers, and supervisors are responsible for safety-related activities across the ATO.

In addition to the responsibilities described above, each operational Service Unit has a Safety Director, which reports directly to the Vice President; a Safety Manager position, which reports directly to the Safety Director, and a Safety Engineer position, which reports to the Safety Manager. For more information regarding Safety Directors, Safety Managers, and Safety Engineers refer to Sections 2.3.6, 2.3.7, and 2.3.8. In addition, the Service Centers were established to provide mission and support services to the Service Units/Areas and are actively involved in SMS implementation.

2.3.6 Safety Director Responsibilities

The Safety Director of each Service Unit is responsible for meeting the competency and training requirements established by Safety Services; facilitating intra- and inter-Service Unit coordination on safety; providing input and advice on safety to the Service Unit Vice President and other leaders; and acting as the Service Unit's liaison with Safety Services.

2.3.7 Safety Manager Responsibilities

Each Service Unit (with the exception of Communications Services and Financial Services) has a Safety Manager who is the management official responsible for safety within the organization and who directly reports to the Service Unit Safety Director. The Safety Managers are responsible for conducting Service Unit safety planning and monitoring; ensuring that the Service Unit meets SMS requirements; and providing support and consultation on safety management within the Service Unit. In some instances, Safety Managers approve certain Safety Risk Management Documents (SRMDs) and accept certain risk. Safety Managers are responsible for facilitating intra- and inter-Service Unit coordination on safety; providing input and advice on safety to the Service Unit Vice President and other leaders; facilitating the integration of SRM into existing processes used to make changes to the NAS; advocating a positive safety culture within the Service Unit; developing and maintaining Service Unit-specific SMS guidance materials and/or requirements, implementation and integration plans; and

cooperating with, and facilitating (as requested) evaluations and audits conducted by Safety Services and/or AOV.

2.3.8 Safety Engineer Responsibilities

Each Service Unit (with the exception of Communications Services and Financial Services) has a Safety Engineer who reports to the Safety Manager to provide SRM technical expertise within the Service Unit. The Safety Engineer's responsibilities include advising the Service Unit Vice President on SMS implementation; supporting, advising, and assisting programs and analysis teams in conducting SRM activities; ensuring the quality and fidelity of the safety analyses within the Service Unit; and if necessary, facilitating the SRM decision process and development of the resulting documentation. Safety Engineers are responsible for providing recommendations to the Safety Manager on SRMD approval; input to the Service Unit Vice President, managers, and directors on risk acceptance; cooperating with and facilitating (as requested) audits conducted by the Safety Services regarding the Service Unit's application of SRM; and coordinating SMS training delivery to Service Unit personnel. Sections 3.13.5 – 3.13.6 further describe the advisory role of Safety Engineers regarding specific types of NAS changes.

The ATO Safety Risk Management Implementation Team (SRMIT) is a group chaired by the Safety Services SRM Manager consisting of FAA Safety Engineers from the Service Units, Service Center, and Safety Services. The purpose of the SRMIT is to promote communication and collaboration across the Service Units throughout the implementation and execution of SMS. The SRMIT provides an environment for the Safety Engineers to effectively communicate best practices, lessons learned, and SMS implementation and execution strategies. The SRMIT develops corporate leadership for the ATO SMS implementation efforts through its function to recommend and review safety policy, guidance, implementation documentation, and training materials. In addition, Safety Engineers participate in both the ATO System Safety Working Group (SSWG) and the ATO Safety Operations Working Group (SOWG). The SSWG reviews SRMDs related to system acquisition changes and the SOWG reviews SRMDs related to operational changes. Sections 3.13.5 – 3.13.6 describe the role of these groups.

Figure 2.1 shows the organizational structure and the primary responsibilities of the Safety Directors, Safety Managers, and Safety Engineers.

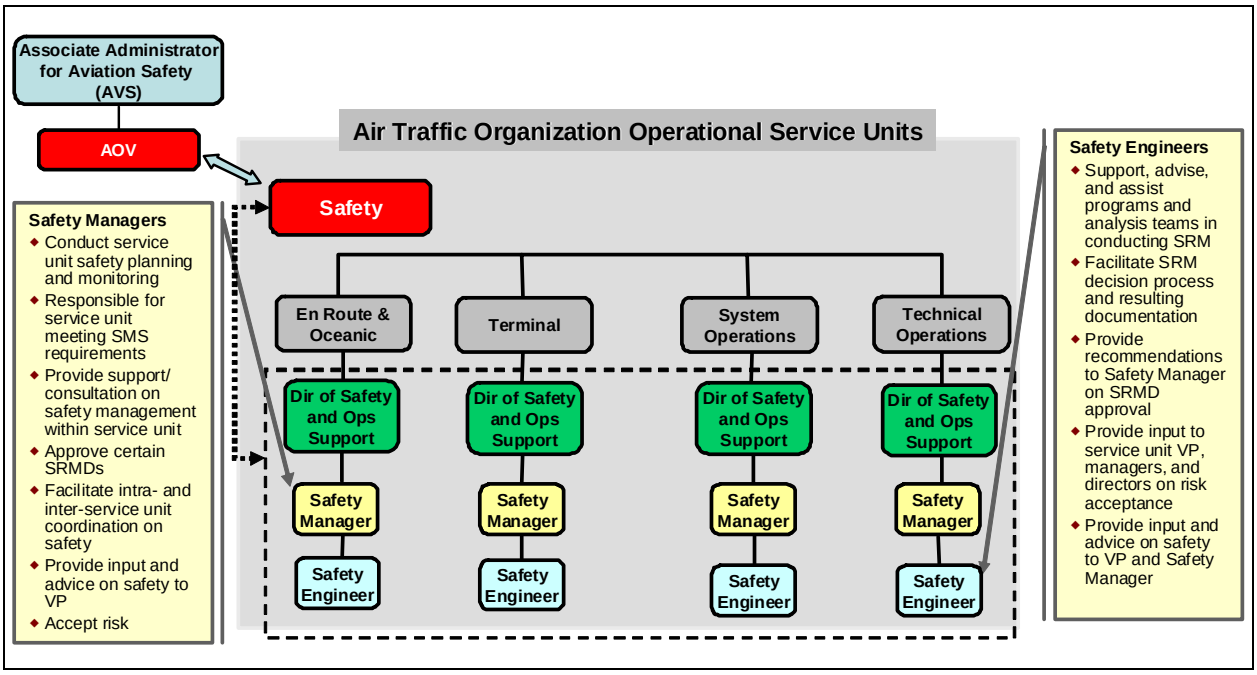


Figure 2.1: Safety Directors, Safety Managers, and Safety Engineers

2.3.9 Associate Administrator for Airports

The Associate Administrator for Airports has been delegated SMS responsibility for ARP functions that impact the safety of the NAS or ATC and navigation services. This includes implementing and complying with the SMS guidance and processes within ARP when ARP impacts NAS safety; ensuring that organizations within ARP's purview cooperate with the ATO implementation of the SMS and integration of SRM into existing processes; providing personnel to serve on SRM Panels and/or provide expertise, as necessary, to allow the ATO to conduct in-depth and complete safety analyses; and requiring that existing orders, policies, directives, and/or guidance within ARP's purview be consistent with the SMS and meet SMS requirements.

2.3.10 Associate Administrator for Aviation Safety

The Associate Administrator for Aviation Safety is responsible for AVS functions that impact the safety of the NAS or ATC and navigation services. These services include implementing and complying with the SMS guidance and processes within AVS as AVS impacts NAS safety; ensuring that organizations within AVS's purview cooperate with the ATO implementation of the SMS and integration of SRM into existing processes; providing personnel to serve on SRM Panels and/or provide expertise, as necessary, to allow the ATO to conduct in-depth and complete safety analyses; requiring that existing orders, policies, directives, and/or guidance within AVS's purview be consistent with the SMS; and providing safety oversight of the ATO through AOV.

2.4 Safety Oversight

2.4.1 Introduction

This section explains safety oversight of the ATO. It describes the responsibilities and authorities of AOV. It also explains the difference between AOV approval and AOV acceptance as well as the items and changes requiring approval and those requiring acceptance.

2.4.2 AOV Oversight Authority

The FAA Administrator created AOV to provide independent safety oversight of the ATO. FAA Order 1100.161, *Air Traffic Safety Oversigh*t, documents this authority; it describes AOV and ATO roles and responsibilities regarding NAS safety. AOV is part of the AVS LOB, which is separate from the ATO. This is in accordance with the ICAO recommendation that, "In those States where the Civil Aviation Authority (CAA) also acts as both the regulator and air traffic service provider, it is important that a clear separation between the air traffic service provision function and the air traffic service safety regulatory function be maintained. The safety regulation of the service provider should be conducted as though the service provider was an external entity in order to maintain the independence of the regulatory function."[8]

AOV has the following responsibilities/authority regarding safety oversight of the ATO:

a. Establish, approve, and/or accept safety standards for the operation and maintenance of the NAS
b. Establish the requirements for the SMS
c. Approve the ATO SMS Manual
d. Monitor ATO compliance with the safety standards and the SMS
e. Audit ATO compliance with the safety standards and the SMS
f. Monitor corrective actions taken by the ATO to ensure identified safety hazards are resolved
g. Provide ATO SMS compliance information to the FAA Administrator
h. Issue safety directives, letters of correction, and/or warning letters to the ATO if it deems such an action necessary or appropriate (in accordance with FAA Order 8000.86, *Air Traffic Safety Oversight Compliance Process*)
i. Review, for concurrence, any proposed responses to safety recommendations from the National Transportation Safety Board (NTSB), the Office of the Inspector General, or Government Accountability Office involving the ATO
j. Review, for concurrence, notifications of differences proposed to be filed by the ATO with ICAO
k. Serve as the primary AVS interface with the ATO on safety issues
l. Share safety data with the ATO

Specific AOV roles related to SRM are described in Chapter 3, *Safety Risk Management*.

2.4.3 Flight Standards Service's Role in Provision of ATC Navigation Services

For the most part, the establishment of AOV does not change Flight Standards Service's (AFS's) role in the provision of ATC and navigation services. Safety-related issues will flow between Safety Services and AOV, while technical issues will continue to flow directly between Service Units and AFS. AFS still approves the following changes, which also require acceptance by AOV:

a. Changes to the following areas of FAA Order 8200.1, *United States Standard Flight Inspection Manual*:
    (1.) Flight inspector's authority and responsibilities
    (2.) Facility status classification and Notices to Airmen (NOTAMs)
    (3.) Records and reports

[8] Eleventh Air Navigation Conference, Montreal, September 22, to October 3, 2003, *The Manual on Safety Management for Air Traffic Services*, *Appendix – Draft Manual on Safety Management for Air Traffic Services*, Chapter 9, Section 9.1.5, p. A-185.

(4.) Extensions in the periodicity or interval of inspections
(5.) Changes in established tolerances or those proposed for new equipment or new functionalities
(6.) Changes in required checklist items for specific areas of systems to be inspected
(7.) Changes in the procedures for evaluating safety and flyability of instrument flight procedures

b. Changes to personnel certification requirements in FAA Order VN 8240.3, *Certification of Flight Inspection Personnel*
c. Changes to the certification standards in FAA Order VN 3330.2, *National Flight Procedures Office (NFPO) Certification Program for Procedures Personnel*

Additionally, AFS continues to provide modeling and analysis support to the ATO for the development of new procedures and separation standards.

2.4.4 AOV and ATO Relationship

In general, Safety Services is the primary interface between AOV and the ATO, as shown in Figure 2.2. Similarly, AOV has agreed to coordinate all ATO interactions through Safety Services. However, AOV may also contact (i.e., audit) the Service Units directly.

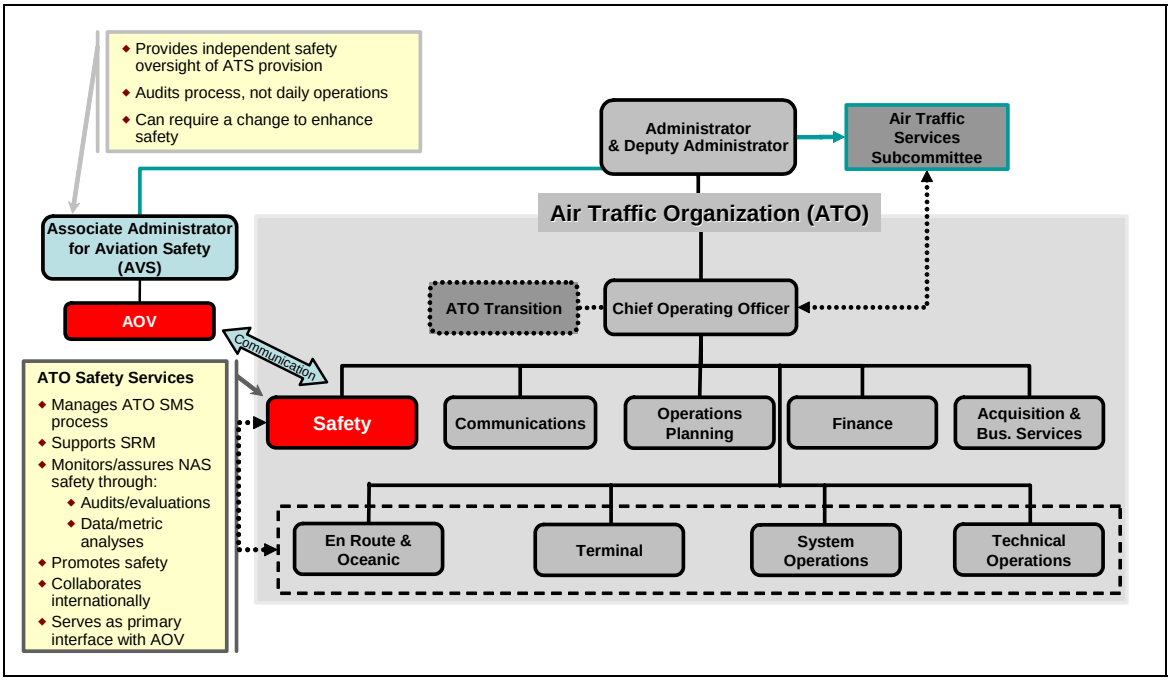


Figure 2.2: AOV/ATO Relationship

2.4.5 AOV Compliance Process

AOV established FAA Order 8000.86, *Air Traffic Safety Oversight Compliance Process,* as a framework to allow it to compel the ATO to correct unsafe conditions. This order describes the process AOV uses to resolve safety compliance issues involving the ATO, excluding those services already regulated by AFS.

Chapter 3 – Safety Risk Management

3.1 Introduction

This chapter describes fundamental SRM concepts, discusses what types of changes are evaluated for safety risk, and details the process and guidance available for determining if a change requires a complete safety analysis under SRM. It also outlines the process of assessing and managing safety risk including:

a. Definitions of commonly used terms
b. Descriptions of safety analysis activities early in the planning or change proposal process
c. Descriptions of the evidence and documentation that indicate that the objectives have been met

This chapter describes the documentation necessary for safety analyses and the required components of the documentation. In addition, it provides information on risk acceptance, document approval, and tracking of changes.

3.2 SRM Overview

3.2.1 How Change Affects Safety

Changes to the NAS create the potential for increased safety risk as the changes interact or interface with existing procedures, systems, or operational environments (e.g., reducing separation minima).

ATO employees use SRM to maintain or improve the safety of the NAS by identifying, managing, and mitigating the safety risk associated with all changes (e.g., changes to systems (hardware and software), equipment, and procedures) that impact safety.

3.2.2 SRM Defined

SRM is a formalized, proactive approach to system safety. SRM is a methodology applied to all NAS changes that ensures that hazards are identified and unacceptable risk is mitigated and accepted prior to the change being made. A **NAS change** is any change to or modification of airspace; airports; aircraft; pilots; air navigation facilities; air traffic control (ATC) facilities; communication, surveillance, navigation, and supporting technologies and systems; operating rules, regulations, policies, and procedures; and the people who implement, sustain, or operate the system components. It provides a framework to ensure that once a change is made, it continues to be tracked throughout its lifecycle.

SRM is a fundamental component of the SMS. It is a systematic, explicit, and comprehensive analytical approach for managing safety risk at all levels and throughout the entire scope of an operation or the lifecycle of a system. It requires the disciplined assessment and management of safety risk.

The SRM process is a means to:

a. Document proposed NAS changes regardless of their anticipated safety impact
b. Identify hazards associated with a proposed change
c. Assess and analyze the safety risk of identified hazards
d. Mitigate unacceptable safety risk and reduce the identified risks to the lowest possible level

e. Accept residual risks prior to change implementation
f. Implement the change and track hazards to resolution
g. Assess and monitor the effectiveness of the risk mitigation strategies throughout the lifecycle of the change
h. Reassess change based on the effectiveness of the mitigations

3.2.3 System, Hazard, and Risk Defined

Three important terms necessary to discuss making NAS changes, the resulting potential hazards, and the management of risk are:

a. **System:** An integrated set of constituent pieces that are combined in an operational or support environment to accomplish a defined objective. These pieces include people, equipment, information, procedures, facilities, services, and other support services.
b. **Hazard:** Any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. A hazard is a condition that is a prerequisite to an accident or incident.
c. **Risk:** The composite of predicted severity and likelihood of the potential effect of a hazard in the worst credible system state. Severity, likelihood, and system state will be defined later in this chapter.

   The system safety methodology, as described in this manual, addresses risk on an individual hazard-by-hazard basis and, therefore, does not address aggregate safety risk. ATO employees determine risk acceptability using the risk matrix in Figure 3.9.

3.2.4 Defenses in Depth: Designing an Error Tolerant System

Given the complex interplay of human, material, and environmental factors in operations, the complete elimination of risk is an unachievable goal. Even in organizations with the best training programs and a positive safety culture, human operators will occasionally make errors;. the best designed and maintained equipment will occasionally fail. System designers take these factors into account and strive to design and implement systems that will not result in an accident due to an error or equipment failure. These systems are referred to as error tolerant. An **error tolerant system** is defined as a system designed and implemented in such a way that, to the maximum extent possible, errors and equipment failures do not result in an incident or accident.

Developing a safe and error tolerant system requires that the system contain multiple defenses allowing no single failure or error to result in an accident. An error tolerant system includes mechanisms that will recognize a failure or error, so that corrective action will be taken before a sequence of events leading to an accident can develop. The need for a series of defenses rather than a single defensive layer arises from the possibility that the defenses may not always operate as designed. This design philosophy is called “defenses in depth.”

Failures in the defensive layers of an operational system can be create gaps in the defenses. As the operational situation or equipment serviceability states change, gaps may occur as a result of:

a. Undiscovered and longstanding shortcomings in the defenses
b. The temporary unavailability of some elements of the system as the result of maintenance action
c. Equipment failure
d. Human error or violation

Design attributes of an error tolerant system include:

a. Making errors conspicuous (error evident systems)
b. Trapping the error to prevent it from affecting the system (error captive systems)
c. Detecting errors and providing warning and alerting systems (error alert systems)
d. Ensuring that there is a recovery path (error recovery systems)

For an accident to occur in a well designed system, these gaps must develop in all of the defensive layers of the system at the critical time when that defense should have been capable of detecting the earlier error or failure. An illustration of how an accident event must penetrate all defensive layers is shown in Figure 3.1.

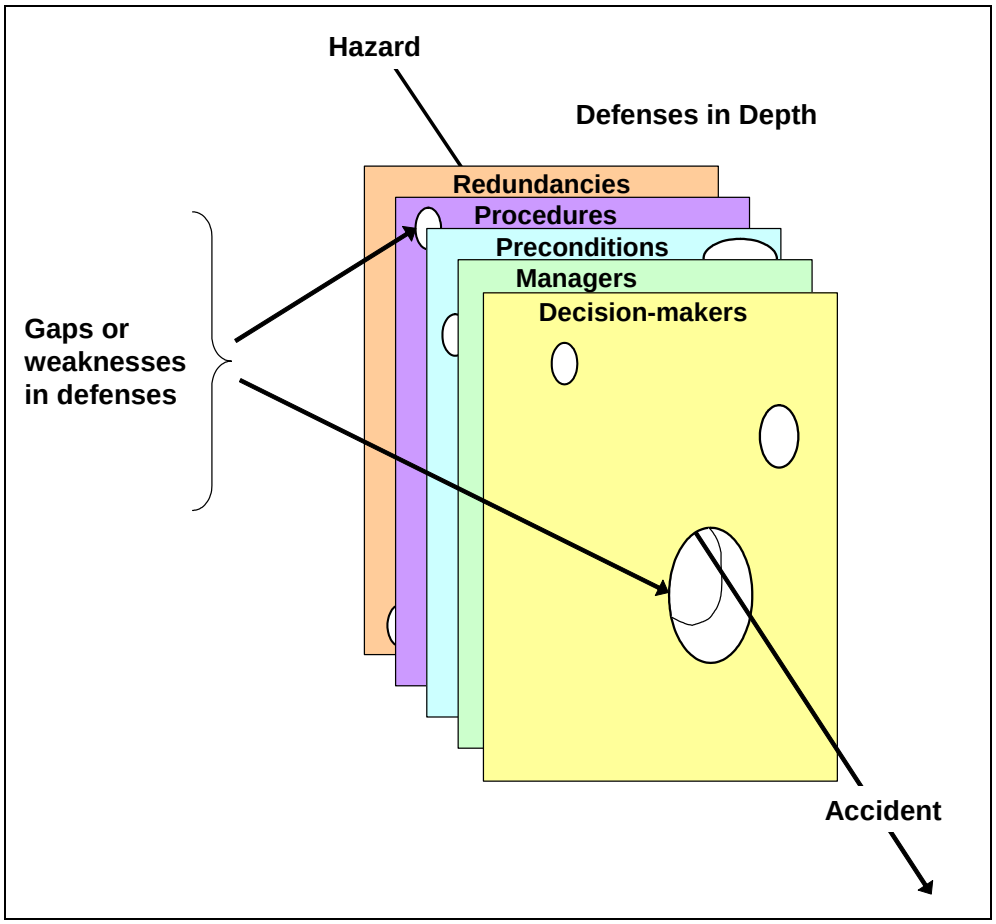


Figure 3.1: Defenses in Depth Philosophy

The gaps in the system's defenses shown in Figure 3.1 are not necessarily static. Gaps "open" and "close" as the operational situation, environment, or equipment serviceability states change. A gap may sometimes be the result of nothing more than a momentary oversight on the part of a controller or operator. Other gaps may represent long-standing latent failures in the system.

A **latent failure** is considered a failure that is not inherently revealed at the time it occurs. For example, when there is a slowly degrading back-up battery that has no state-of-charge sensor, the latent failure would not be identified until the primary power source failed and the back-up

battery was needed. If no maintenance procedures exist to periodically check the battery, the failure would be considered an undetected latent event.

3.2.5 Detecting Gaps

The task of reducing risk can be applied in both proactive and reactive ways. Careful analysis of a system and operational data monitoring make it possible to identify sequences of events where faults and errors (either alone or in combination) could lead to an incident or accident before it actually occurs. The same approach to analyze the chain of events that lead to an accident can also be used after the accident occurs. Identifying the active and latent failures revealed by this type of analysis enables one to take corrective action to strengthen the system's defenses.

3.2.6 Closing Gaps

The following examples of typical defenses used in combination to close gaps are illustrative and by no means a comprehensive list of solutions:

<u>Equipment</u>

a. Redundancy
   (1.) Full redundancy providing the same level of functionality when operating on the alternate system
   (2.) Partial redundancy resulting in some reduction in functionality (e.g., local copy of essential data from a centralized network database)
b. Independent checking of design and assumptions
c. System designed to ensure that a critical functionality is maintained in a degraded mode in the event that individual elements fail
d. Policy and procedures regarding maintenance, which may result in loss of some functionality in the active system or loss of redundancy
e. Automated aids or diagnostic processes designed to detect system failures or processing errors and report those failures appropriately
f. Scheduled maintenance

<u>Operating Procedures</u>

a. Adherence to standard phraseology and procedures
b. Readback of critical items in clearances and instructions
c. Checklists and habitual actions (e.g., requiring a controller to follow through the full flight path of an aircraft, looking for conflicts, receiving immediate coordination from the handing-off sector)
d. Inclusion of a validity indicator in designators for Standard Instrument Departures and standard terminal arrival routes
e. Training, analyses, and reporting methods

<u>Organizational Factors</u>

a. Management commitment to safety
b. Current state of safety culture
c. Clear safety policy
   (1.) Implemented with adequate funding provided for safety management activities

d. Oversight to ensure correct procedures are followed
   (1.) No tolerance for willful violations or shortcuts
e. Adequate control over the activities of contractors

For information on the preferred order for developing risk mitigation controls, refer to Table 3.5 in Section 3.11.9.

3.2.7 Effect of Hardware and Software on Safety

System designers generally design the hardware and software components of a system to meet specified levels of reliability, maintainability, and availability. The techniques for estimating system performance in terms of these parameters are well established. When necessary, system designers can build redundancy into a system, to provide alternatives in the event of a failure of one or more elements of the system.

Designers use system redundancy and hardware and/or software diversity to provide service in the event of primary system failures. Different hardware and software meet the functional requirements for the back-up mode.

Physical diversity is another method system designers use to increase the likelihood of service availability in the event of failures. Physical diversity involves separating redundant functions so that a single point of failure does not corrupt both paths, making the service unavailable. An example of physical diversity is the requirement to bring commercial power into Air Route Traffic Control Centers (ARTCCs) through two different locations. In the event of a fire or other issue in one location, the alternate path would still provide power, which increases the likelihood that service would remain available.

When a system includes software and/or hardware, the safety analyses consider possible design errors and the hazards they may create. Systematic design processes are an integral part of detecting and eliminating design errors.

3.2.8 Human Element's Effect on Safety

Ultimately, every system within the NAS exists to assist a human in task performance. Therefore, system designers must design the human-to-the-system interface and associated procedures to capitalize on human capabilities and to compensate for human limitations. One limitation is human performance variability, which necessitates careful and complete analysis of the potential impact of human error. Machines and systems are built to function within specific tolerances, so that identical machines have identical, or nearly identical, characteristics. By contrast, humans vary due to genetic and environmentally determined differences. Designers take these differences into account when designing products, tools, machines, and systems to "fit" the target user population. Human capabilities and attributes differ in areas such as:

a. Sense modalities (manner and ability of the senses, (e.g., seeing, hearing, touching))
b. Cognitive functioning
c. Reaction time
d. Physical size and shape
e. Physical strength

Fatigue, illness, and other factors such as stressors in the environment, noise, and task interruption also impact human performance. Designers use Human Error Analysis (HEA) to identify the human actions in a system that can create hazardous conditions. Optimally, the

system is designed to resist human error (error resistant system) or at a minimum, to tolerate human error (error tolerant system).

Human error is estimated to have been a causal factor in 60 to 80 percent of aviation accidents and incidents and is directly linked with system safety, error, and risk.[9] People make errors, which have the potential to create hazards. Accidents and incidents often result from a chain of independent errors. For this reason, system designers must design safety-critical systems to eliminate as many errors as possible, minimize the effects of errors that cannot be eliminated, and lessen the negative impact of any remaining potential human errors.

Within the FAA, **human factors** is defined as a "multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to equipment, systems, facilities, procedures, jobs, environments, training, staffing and personnel management for safe, comfortable, effective human performance" (FAA Order 9550.8, *Human Factors Policy*).

Human factors examines the human role in a system or application (e.g., hardware, software, procedure, facility, document, other entity) and how the human is integrated into the design. Human factors applies knowledge of how humans function in terms of perception, cognition, and biomechanics to the design of tools, products, and systems that are conducive to human task performance and protective of human health and safety.

When examining adverse events attributed to human error, often elements of the human-to-system interface (such as display design, controls, training, workload, or manuals and documentation) are flawed. Human reliability analysis and the application of human performance knowledge must be an integral part of the SMS; affecting system design for safety-critical systems. Recognizing the critical role that humans and human error play in complex systems and applications has led to the development of the human-centered design approach. This human-centered design approach is central to the concept of managing human errors that affect safety risk.

3.3 Applicability of SRM

3.3.1 Items Requiring Evaluation for Safety Risk

All proposed changes to the NAS (e.g., new equipment; systems; modifications to existing equipment, systems and new and/or changes to existing procedures; operations) require SRM evaluation, in accordance with ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*, and this manual. FAA Order 1100.161, *Air Traffic Safety Oversight*, specifically cites the following categories of changes as requiring a safety analysis:

a. Airspace changes that impact safety, including:
   (1.) Reorganization of air traffic route structure
   (2.) Resectorization of an airspace
b. Changes to air traffic procedures and standards that impact safety, including:
   (1.) Reduced separation minima applied to airspace
   (2.) New operating procedures, including departure, arrival, and approach procedures
   (3.) Waivers to existing procedures, requirements, or standards

[9] Shappell, S.A, Wiegman, D.A., *A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System*, Ashgate Publishing, Ltd., 2003

c. Changes to airport procedures and standards that impact safety, including:
   (1.) Reduced separation minima applied at an airport
   (2.) Physical changes to airport runways, taxiways, or the airport operations area
d. Changes to equipment that impact safety, including:
   (1.) Introduction of new equipment, systems (hardware and software) that impact safety, human-to-system interfaces, or facilities used in providing ATC and navigation services
   (2.) Modifications to systems (hardware and software), maintenance activities associated with those systems, human-to-system interfaces, or facilities used in providing ATC and navigation services

Since many established operations, procedures, and routine maintenance actions pre-date the implementation of the SMS, they were not evaluated under the purview of the SRM process described in this manual. AOV accepted the NAS as it existed when FAA Order 1100.161, *Air Traffic Safety Oversight*, was signed on March 14, 2005, as the baseline. AOV SOC 07-01, *Acceptance of the Air Traffic Organization (ATO) Baseline*, states that "from that point forward [March 14, 2005], the use of SRM to assess all changes to the NAS was established, with the goal of full SMS implementation by March 14, 2010."

Figure 3.2 provides an overview of SRM and the NAS.

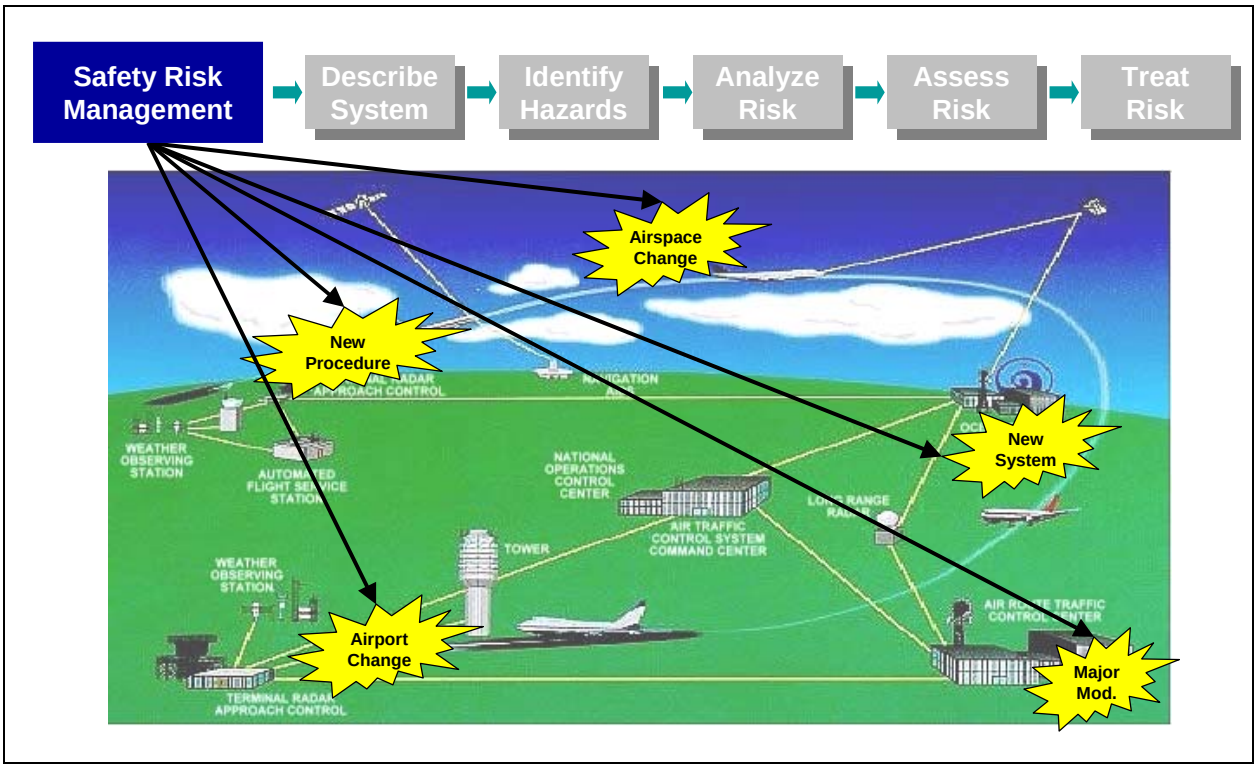


Figure 3.2: SRM and the NAS

3.4 Planning

3.4.1 Planning SRM

Planning the SRM effort requires that one:

a. Decides the level and type of safety analysis that is needed
b. Coordinates with other organizations that may be affected by the change or the risk mitigation strategies

The scope of the SRM effort is a function of the nature, complexity, and impact or consequence of the change. It is critical that the scope and complexity of the safety analysis match the scope and complexity of the change. To support this activity, the originating organization should consult its Safety Engineer to determine if SOWG and/or SSWG involvement is needed.

It is important for the SRM Panel to recognize how systems or items initially determined to have no impact on safety could potentially impact the system or change being analyzed. For instance, air conditioning may not initially appear to have an impact on NAS safety; however, when a system depends on air conditioning to keep it from overheating and failing, air conditioning (or lack thereof) could impact the safety of that system, as well as the safety of the NAS. Issues or potential hazards captured through the SRM process/analysis, but not directly the result of the change being assessed, must be formally passed or transferred onto the appropriate party by following the Documenting Existing Hazards process discussed in Section 3.8.4.

3.4.2 SRM Panel

An SRM Panel should include representatives and stakeholders from the various organizations affected by the change. It is important that the panel be made up of an appropriately diverse team, including stakeholders and experts, who will be involved, in different capacities, throughout the safety analysis process. A **stakeholder** is a group or individual that is affected by or is in some way accountable for the outcome of an undertaking; an interested party having a right, share, or claim in a product or service, or in its success in possessing qualities that meet that party's needs and/or expectations.[10]

Though the size and make-up of the panel will vary with the type and complexity of the proposed change, involving the following types of expertise on the SRM Panel should be considered (list not all-inclusive):

a. Employees directly responsible for developing the proposed change
b. Employees with current knowledge of and experience with the system or change
c. Hardware and/or software engineering or automation expert to provide knowledge on equipment performance
d. SRM specialist to guide the application of the methodology
e. Human factors specialist
f. Software specialist
g. Systems specialist
h. Employees skilled in collecting and analyzing hazard and error data and using specialized tools and techniques (e.g., operations research, data, human factors, failure mode analysis)

[10] Definition from the *The Federal Aviation Administration Integrated Capability Maturity Model (FAA-iCMM)*, Version 2.0

3.4.3 Panel Facilitator Responsibilities

For each SRM Panel, there should be one person who serves as the SRM Panel facilitator. The facilitator or a member of the SRM Panel collects information relevant to the change. This information may include meeting with the person who proposed the change. The change proponent must clarify the:

a. Current system state or condition
b. Proposed change
c. Intent of the change
d. System state(s) in which the change will be conducted
e. Boundaries of the analysis
f. Assumptions that may influence the analysis

The SRM Panel facilitator ensures that the following occurs:

a. Potential panel members are identified.
b. Panel members have a common understanding of the SMS and SRM principles.
c. Material required for the first meeting is gathered, including:
   (1.) Preliminary Hazard Lists (PHLs) of similar changes
   (2.) Collection and analysis of data appropriate to the change to assist in hazard identification and risk assessment
   (3.) SRM handouts (severity and likelihood table and risk matrix)
d. Panel members are aware of meeting logistics.
e. Co-facilitator is identified (co-facilitator will later work with the facilitator and the change proponent to help prepare the final safety document).
f. SRM Panel orientation is prepared (i.e. why we are here, what are we trying to accomplish, what is our schedule, etc.).
g. Initial set of SRM Panel ground rules are developed (i.e. how the panel members will interact with each other).

At the initial meeting, the facilitator must present a panel orientation, including:

a. Summary of the goals and objectives for the panel
b. Brief review of the SRM process
c. Development of SRM Panel ground rules
d. Determination of how often the SRM Panel will meet along with location, time, and date
e. Presentation of the proposed change with the sample PHL data and other information pertinent to the change

Involving panel members with varying experience and knowledge leads to a broader, more comprehensive, and more balanced consideration of safety issues than an individual assessment. The following is a recommended process for the SRM Panel:

a. Individuals use the group session to generate ideas and undertake preliminary assessment only (perhaps identifying factors that are important, rather than working through the implications in detail).
b. A subset of the panel with sufficient breadth of expertise to understand all the issues raised and a good appreciation of the purposes of the assessment, collate and analyze the findings after the session. The person who facilitated or recorded the session often is most able to perform this task.

c. The individuals who collate and analyze the results present them to the group to check that input has been correctly interpreted. This also gives the group a chance to reconsider any aspect once they can see the whole picture.

3.4.4 Involving AOV During Safety Analysis

FAA Order 1100.161, *Air Traffic Safety Oversight,* stipulates that certain types of changes require either AOV approval or AOV acceptance. As such, an SRM Panel should evaluate the proposed change to determine whether it will require approval or acceptance from AOV (defined below). If so, the SRM Panel should coordinate with its Service Unit Safety Engineer(s), who will liaise with Safety Services to involve AOV at the early planning stages of the safety analysis as outlined in AOV SOC 07-02, *AOV Concurrence/Approval at Various Phases of Safety Risk Management Documentation and Mitigations for Initial High-Risk Hazards* and AOV SOC 07-05, *AOV Guidance on Safety Risk Modeling of High Risk Hazards*.

a. **AOV Approval:** The formal act of responding favorably to a change submitted by a requesting organization. This action is required prior to the proposed change being implemented.
b. **AOV Acceptance:** The process whereby the regulating organization has delegated the authority to the service provider to make changes within the confines of approved standards and only requires the service provider to notify the regulator of those changes within 30 days. Changes made by the service provider in accordance with its delegated authority can be made without prior approval by the regulator.

3.4.5 Items Requiring AOV Approval

The following items require AOV approval prior to implementation:

a. The ATO SMS Manual and any changes made to it
b. Controls that are defined to mitigate or eliminate initial or current high risk hazards
c. Changes or waivers to provisions of handbooks, orders, and documents, including FAA Order 7110.65, *Air Traffic Control* that pertains to separation minima
d. The NAS equipment availability program and any changes to the program

All items submitted to AOV for approval first require Service Unit approval, then approval by Safety Services.

3.4.6 Items Requiring AOV Acceptance

The following items or changes require acceptance by AOV:

a. Exclusions to SMS requirements granted by Safety Services
b. Changes to criteria in FAA Order 8200.1, *United States Standard Flight Inspection Manual*
   (1.) Flight inspector's authority and responsibilities
   (2.) Facility status classification and issuance of NOTAMs
   (3.) Records and reports
   (4.) Extensions in the periodicity or interval of inspections
   (5.) Changes in established tolerances or those proposed for new equipment or new functionality
   (6.) Changes in required checklist items for specific areas of systems to be inspected
   (7.) Changes in the procedures for evaluating safety and flyability of instrument flight procedures

c. Changes to personnel certification requirements in FAA Order VN 8240.3, *Certification of Flight Inspection Personnel*
d. Changes to the certification standards in FAA Order VN 3330.2, *National Flight Procedures Office (NFPO) Certification Program for Procedures Personnel*
e. Changes to certification criteria in paragraph 504 of FAA Order 6000.15, *General Maintenance Handbook for National Airspace System (NAS) Facilities*
f. Changes to the personnel certification requirements in FAA Order 3400.3, *Airway Facilities Maintenance Personnel Certification Program*
g. Mitigations/controls in cases in which safety risk and/or controls/mitigations are outside of the ATO (i.e., ARP and/or AVS); the mitigations are also approved by the designated management officials within each affected LOB

3.5 Preliminary Safety Analysis

3.5.1 Required Levels of Safety Analysis

Figure 3.3 describes the process for determining what type of safety analysis is required under SRM.

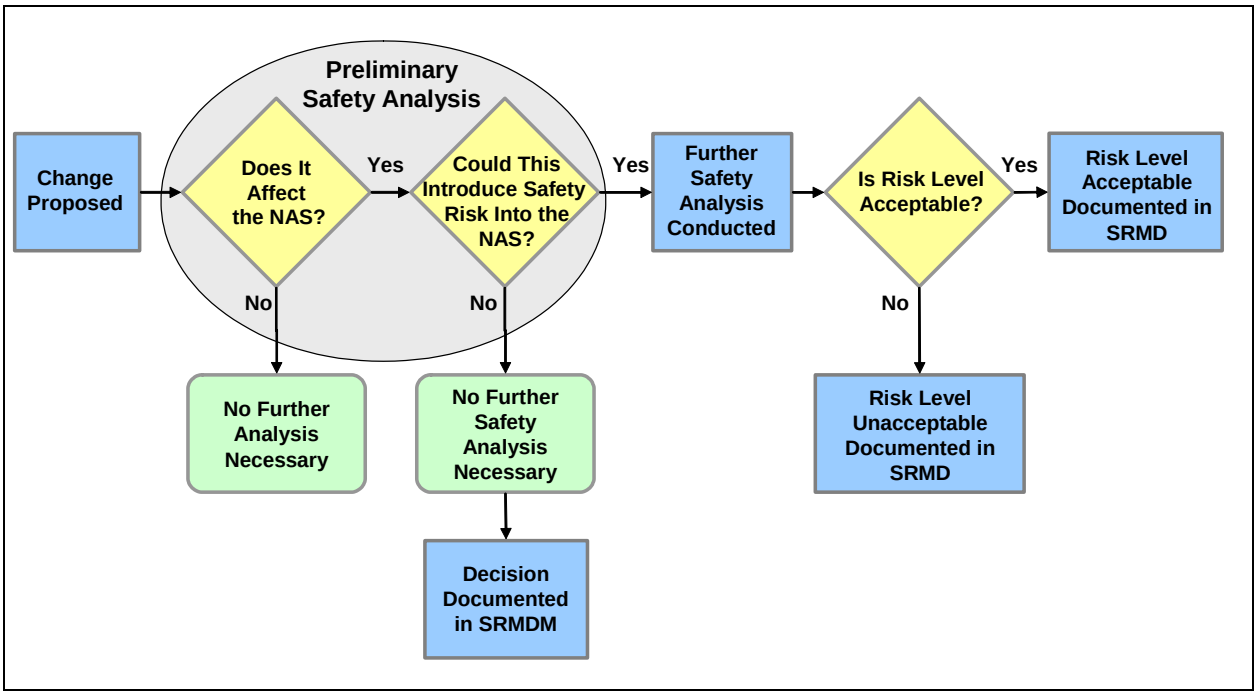


Figure 3.3: SRM Decision Process

When proposing a change to the NAS, change proponents must perform a preliminary safety analysis. If the change does not affect the NAS, there is no need to conduct a further safety analysis. If the change does affect the NAS, a fundamental question to ask is: does the change have the potential to introduce safety risk into the NAS? Additional questions to make that determination may include:

a. Does the change affect pilot and controller interaction?
b. Does the change affect existing controller processes or procedures?

c. Does the change represent a change in operations (either air traffic service or system maintenance)?
d. Does the change modify the form, fit, and/or function of a critical NAS system?

If the change is not expected to introduce safety risk into the NAS, there is no need to conduct further safety analysis; instead, the change proponent documents that determination, along with the justification for the decision as to why the change is not subject to the provisions of additional SRM assessments and supporting documentation beyond the initial safety analysis in an SRM Decision Memo (SRMDM), described in Section 3.5.2. If the change is expected to impact the safety of the NAS, it is necessary to conduct further safety analysis and document the safety analysis in an SRMD. Even when a change is proposed to improve safety, the need to conduct further safety analysis remains.

The level at which an organization conducts SRM varies by organization, change proponent, and/or type of change. In some cases, SRM Panels will perform SRM at the national level, and in other cases, panels will perform SRM at the Service Area or local level. Not all changes affect the NAS or require further safety analysis. Figure 3.4 provides a spectrum of NAS change examples.

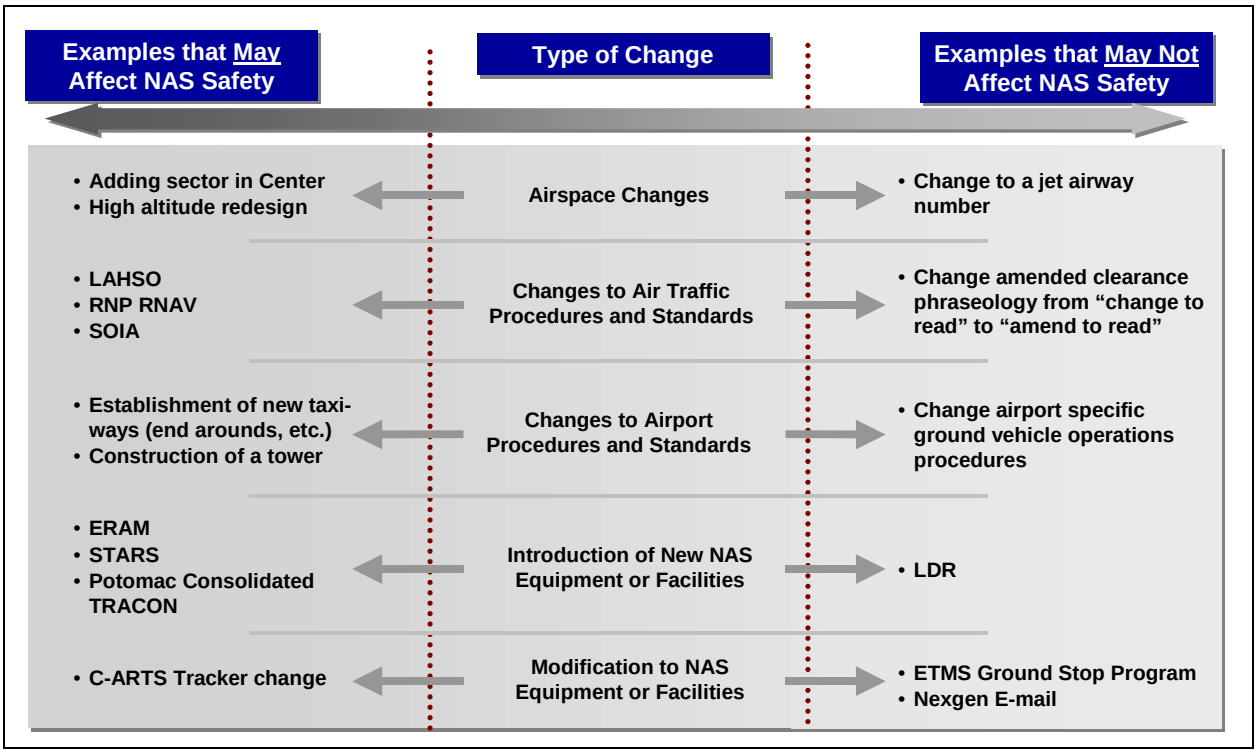


Figure 3.4: Spectrum of NAS Change Examples

3.5.2 SRMDM: No Safety Risk Introduced to the NAS

In the early stages of analysis, it may become evident that a change does not introduce any safety risk into the NAS. In this case, there is no need to further assess the safety risk. The SRMDM was adopted by the ATO to document all proposed NAS changes that do NOT introduce any safety risk (hazards) to the NAS. This determination may be made by the change proponent, affected Service Unit(s), or SRM Panel. The SRMDM must include a description of the proposed change and the justification for the decision that the change is not subject to the provisions of additional SRM assessments, and supporting documentation beyond the preliminary safety analysis. The justification must describe the rationale supporting the finding that the proposed change does NOT introduce any safety risk to the NAS. All SRM documentation, including SRMDMs, must be kept on file throughout the lifecycle of a system or change.

An SRMDM is required to have two signatures at a minimum, one from the change proponent and one from a designated management official of the affected Service Unit. Service Units may employ additional signatory requirements. Each Service Unit Safety Engineer can provide Service Unit specific guidance.

SRMDMs on programs included as FAA's Capital Investment Programs, those defined by OMB Circular A-11, part 7, Exhibit 300, or those specifically designated by the Service Unit or Safety Services require two additional signatures and must adhere to the guidance outlined in the *Safety Risk Management Guidance for System Acquisitions* (SRMGSA). These SRMDMs must be reviewed by the affected Service Unit(s) Safety Engineer(s) and the Chairperson of the ATO SSWG must concur.

Additionally, Appendix E, *SRMDM Template*, provides specific guidance for developing an SRMDM and an SRMDM template. Appendix F, *SRMDM Review Checklist*, contains criteria by which SRM Panels can evaluate the completeness of an SRMDM.

3.6 When Further Safety Analysis Is Required

3.6.1 SRM Safety Analysis Phases

Consistent with ICAO guidelines and best practices, the SRM phases in Figure 3.5 are equally applicable to any SRM activity, whether it pertains to operations, maintenance, procedures, or new system development. Figure 3.6 illustrates how the five phases of the SRM safety analysis are accomplished. Systematically completing these steps creates a thorough and consistent safety analysis.

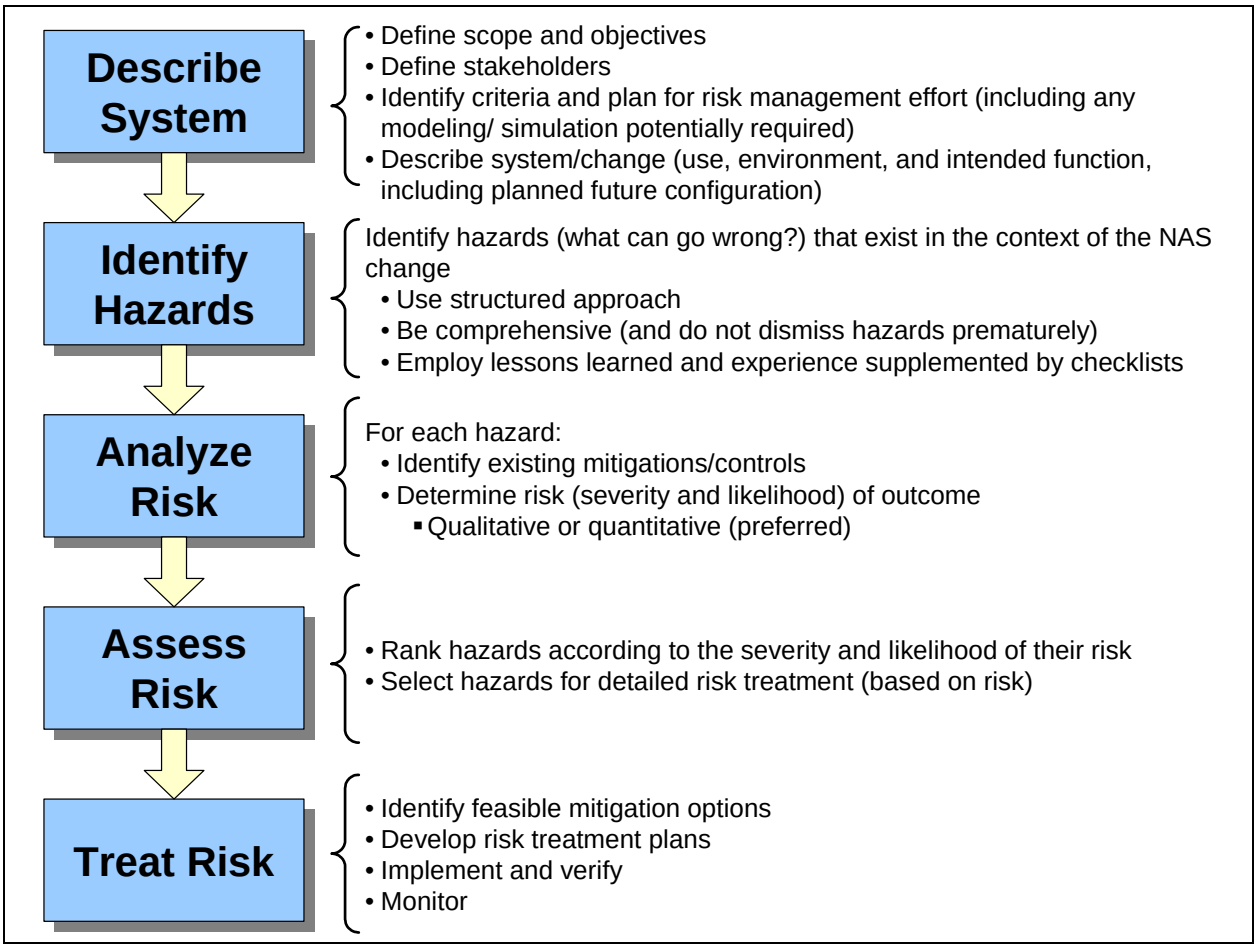


Figure 3.5: SRM Safety Analysis Phases

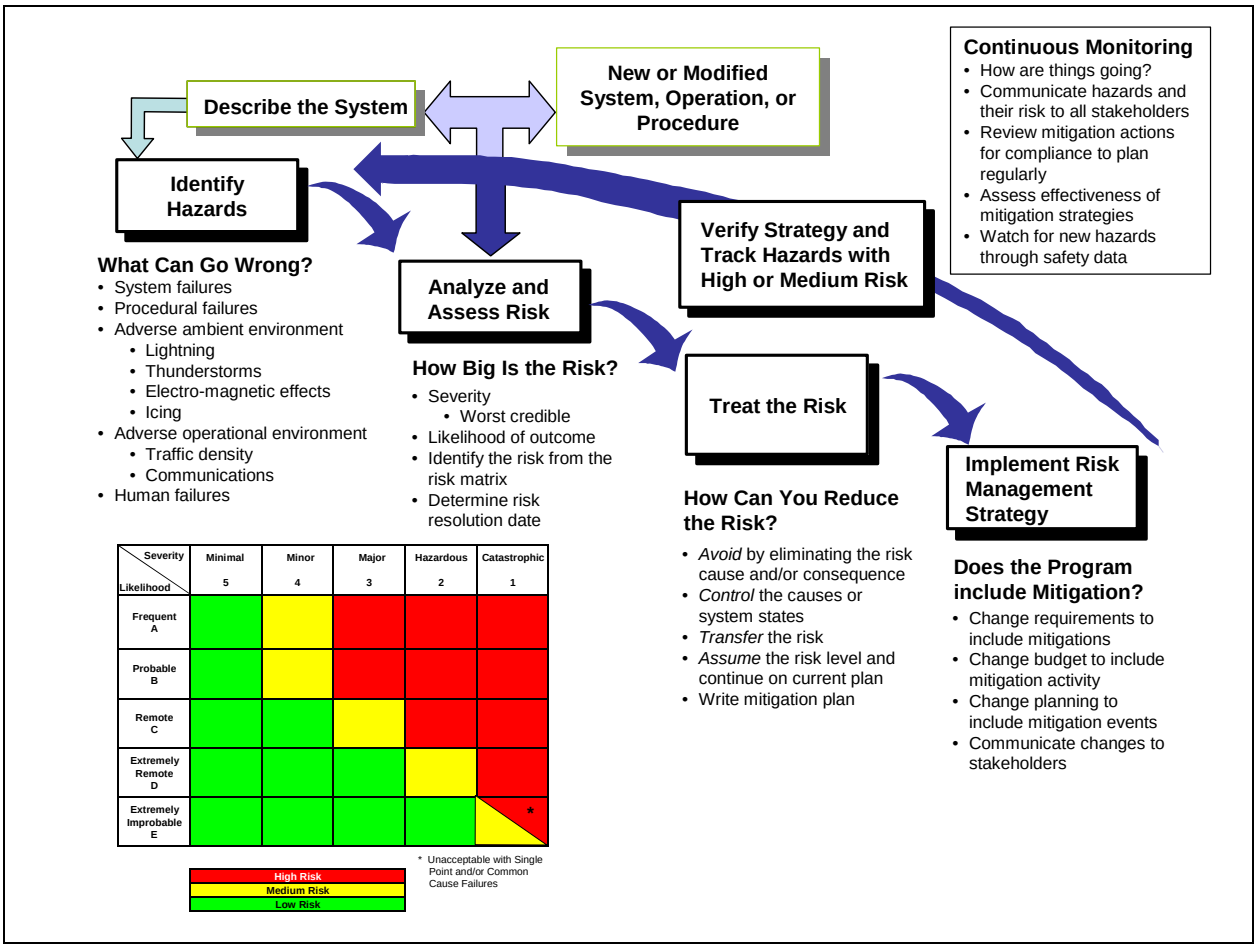


Figure 3.6: How to Accomplish a Safety Analysis

The safety steps are closed-loop, meaning those tasked with executing SRM repeat one or more steps until the safety risk for each hazard is acceptable. Regardless of the phase of operation, these steps assist SRM practitioners in identifying and managing the safety risk associated with providing ATC and navigation services.

3.7 Phase 1: Describe System

3.7.1 Describing the System

A good system description is the critical foundation for conducting a sound safety analysis. The system description provides information that serves as the basis to identify all hazards and associated safety risks. It is critical that the SRM Panel members:

a. Define and document the scope and objectives of the proposed change or system
b. Describe and model the system and operation in sufficient detail for the safety analysis to proceed to the next stage—identifying hazards (e.g., modeling might entail creating a functional flow diagram to help depict the system and the interface with the users, other systems, or sub-systems)

c. Are aware that the system is always a sub-component of some larger system. For example, even if the analysis encompasses all services provided within an entire ARTCC, it can be considered a subset of a larger body of airspace, which in turn, is a subset of the NAS.

3.7.2 Potential Effects on the System or Interfacing Systems

This phase considers all critical factors. The resulting description defines the scope of the risk assessment. A complete and accurate system description is the essential foundation for conducting a thorough safety analysis. System descriptions need to exhibit two essential characteristics—correctness and completeness.

a. Correctness in a description means that it accurately reflects the system without ambiguity or error.
b. Completeness means that nothing has been omitted and that everything stated is essential and appropriate to the level of detail.

A description of the change may be a full report or a paragraph; length is not important, as long as the description covers all of the essential elements. It is vital that the description of the proposed change be correct and complete. If the description is too vague, incomplete, or otherwise unclear, it must be clarified before continuing the safety analysis. Questions to consider include:

a. What is the purpose of the system or change?
b. How will the system or change be used?
c. What are the system or change functions?
d. What are the system or change boundaries and external interfaces?
e. What is the environment in which the system or change will operate?
f. What are the interconnectivity and/or interdependencies between systems?
g. How will the change impact system users?

The following are examples of data that the people conducting the safety analysis could consider when describing the system:

a. Average annual approaches to each runway
b. Number of hours the airport is at or below minimums
c. Number and type of airport operations
d. Number of aircraft controlled, ground, pattern, Instrument Flight Rules (IFR), Visual Flight Rules (VFR), and transitions
e. Number of hours the airport is in VFR vs. IFR
f. Availability and reliability for both hardware and software
g. Number of pilot deviations
h. Number of Operational Errors/Operational Deviations
i. Number of pedestrian/vehicle deviations
j. Accident/injury data

Chapter 4, *Safety Assurance*, provides potential sources for data to be used in SRM.

3.7.3 5M Model of System Description

SRM Panels can use a variety of methods to create a system description. The 5M Model shown in Figure 3.7 is one useful method to capture the information needed to describe the system.

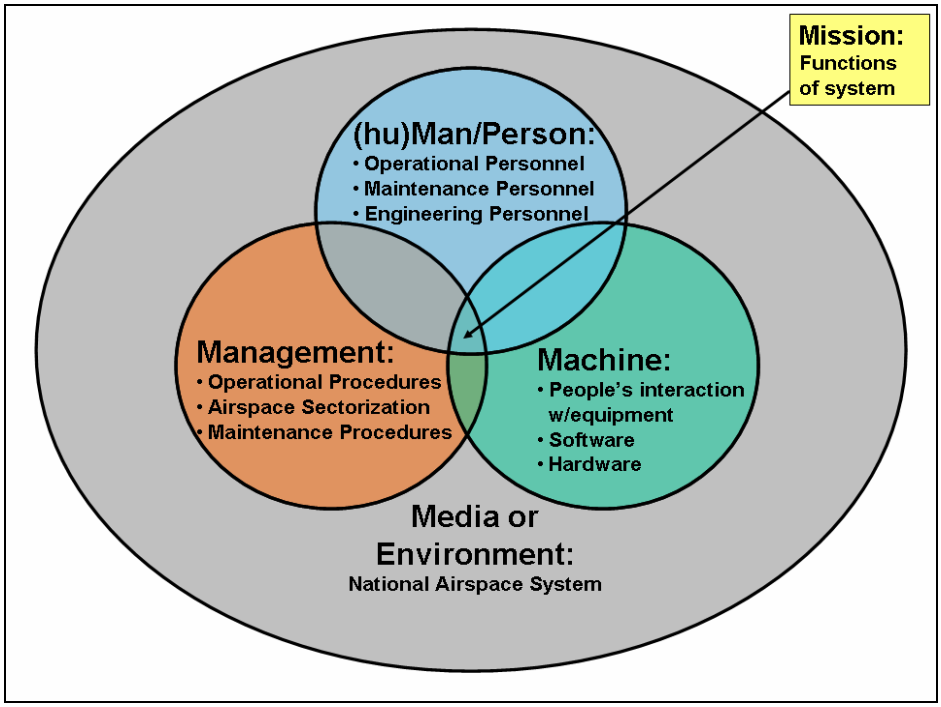


Figure 3.7: 5M Model

The 5M Model illustrates five integrated elements in any system:

a. **Mission** – The functions that the system needs to perform
b. **(hu)Man/person** – The human operators and maintainers
c. **Machine** – The equipment used in the system including hardware, firmware, software, human-to-system interface, and avionics
d. **Management** – The procedures and policies that govern the system's behavior
e. **Media** – The environment in which the system is operated and maintained

The 5M Model and similar techniques are used to deconstruct the proposed change to distinguish elements that are part of, or impacted by, the proposed change. These elements later help to identify sources, causes, hazards, and current and proposed hazard mitigations.

3.7.4 Bounding the System: Limit Analysis to Scope of the Change

Bounding is limiting the analysis of the change or system to the elements that affect or interact with each other to accomplish the central function. The level of detail in the description varies, typically proportionally to the breadth of the change. The system description has both breadth and depth. Breadth refers to the system boundaries, and depth refers to the level of detail in the description. A thorough system description and the elements within it constitute the potential sources of hazards associated with the proposed change. This is critical to the subsequent phases of the SRM process.

The resulting bounded system description limits the analysis to the components necessary to adequately assess the safety risk associated with the change.

3.7.5 Required Depth and Breadth of the Analysis

The depth and breadth of the analysis necessary for SRM varies. Some of the factors used to determine the depth and breadth of the analysis include:

a. **The size and complexity of the change under consideration** – A larger and more complex change may also require a larger and more complex analysis.
b. **The breadth of a change** – SRM scope can be expected to increase if the change spans more than one organization or LOB.
c. **The type of change** – Procedural- or equipment-driven changes tend to require more analysis than a frequency change.

Selecting the appropriate scope and detail of the safety analysis is critical; the SRM Panel takes multiple factors into consideration when making these determinations. In general, safety analyses on more complex and far-reaching changes will require a greater scope and detail. For example, a major acquisition program could require multiple safety analyses involving hundreds of pages of data at the preliminary, sub-system, and system levels, evaluating numerous interfaces with other systems, users, and maintainers in the NAS. However, an operational procedure change at an Air Traffic Control Tower (ATCT) may require a less intensive analysis that describes the change and identifies the hazards and associated risks. In both cases, the SRM requirements are met, but the safety analysis is tailored to meet the needs of the decision-makers.

A primary consideration in determining both scope and detail of the safety analysis is: What information is required to know enough about the change, the associated hazards, and each hazard's associated risk to choose which controls to implement and whether to accept the risk of the change? The scope of the analysis enables making an informed decision about whether the proposed change is acceptable for implementation from a safety perspective. If there is doubt about whether to include a specific element in the analysis, it is better if the panel includes that item at first, even though it might prove irrelevant during the hazard identification phase.

Guidelines to help determine the scope of the SRM effort include:

a. Sufficient understanding of system boundaries to encompass possible impacts the system could have, including interfaces with peer systems, larger systems of which it is a component, and users and maintainers
b. System elements
c. Limiting the system to those elements that affect or interact with each other to accomplish the mission or function

At a minimum, the safety analysis should detail the system and its hazards so that the projected audience can completely understand the associated safety risk. Guidelines that help determine depth include:

a. More complex and/or increased quantity of functions will increase the number of hazards and related causes.
b. Complex and detailed analyses will explore multiple levels of hazard causes, sometimes in multiple safety analyses.
c. Hazards that are suspected to have associated initial high or medium risk should be thoroughly analyzed for causal factors and likelihood.
d. The analysis should be conducted at a level that can be measured or evaluated.

3.8 Phase 2: Identify Hazards

3.8.1 Identifying Hazards

Once the SRM Panel has completely and accurately described the system (Phase 1), it can identify hazards. A **hazard** is defined as any real or potential condition that can result in injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. A hazard is a condition that is a prerequisite to an accident or incident.

A thorough system description and the elements within it constitute the potential sources of hazards associated with the proposed change. During the hazard identification phase, the panel identifies and documents potential safety issues, their possible causes, and corresponding effects. The level of detail required in the hazard identification process depends on the complexity of the change being considered and the stage at which the SRM Panel is performing the analysis. A more comprehensive hazard identification process leads to a more rigorous safety analysis.

3.8.2 Elements of Hazard Identification

In the identify hazards phase, the SRM Panel identifies hazards to the system (i.e., operation, equipment, and/or procedure) in a systematic way. There are numerous ways to do this, but all require at least three elements:

a. Operational expertise
b. Training or experience in various hazard analysis techniques
c. A defined hazard analysis tool

The SRM Panel defines the data sources and measures necessary to identify hazards and to monitor for compliance with mitigation strategies. Data monitoring also helps detect hazards that are more frequent or more severe than expected or mitigation strategies that are less effective than expected. Whoever performs the hazard analysis selects the tool that is most appropriate for the type of system being evaluated. Table 3.1 in Section 3.8.6 lists several hazard identification and analysis tools and techniques with descriptions and references. These are just some of the many tools that panels can use to identify hazards. Appendix G, *Hazard Identification and Analysis Tools and Techniques,* provides additional information on each tool or technique. If unsure about which tool to use, or how to use any of them, panel members should consult their Service Unit Safety Engineer(s) for guidance.

3.8.3 Potential Sources of Hazards

The hazard identification stage considers all of the possible sources of hazards. Depending on the nature and size of the system under consideration, these could include:

a. Equipment (hardware and software)
b. Operating environment (including physical conditions, airspace, and air route design)
c. Human operators
d. Human-machine interface
e. Operational procedures
f. Maintenance procedures
g. External services

The SRM Panel should refer to the system description it created using the 5M Model or other technique. These elements are often the sources for hazards.

3.8.4 Documenting Existing Hazards

The Documenting Existing Hazards Process describes the documentation and notification actions required when an existing hazard is identified. During Phase 2 of the SRM process, the SRM Panel or change proponent identifies hazards for the NAS change undergoing the analysis. Those hazards fall into three categories:

a. Pre-existing hazards *not in* scope and *not caused* by the change
b. Pre-existing hazards *in scope* and *not caused by* the change
c. Hazards *in scope* and *caused by* the change

Each of these three categories follows a specific process for ensuring ownership, documentation, and monitoring. These steps are described in detail in Appendix H, *Documenting Existing Hazards Process*.

The overall objective of the SMS is to improve NAS safety. There may be instances in which a panel discovers existing high risk hazards through an assurance program, a safety analysis, or other means. In those cases, corrective action is necessary to resolve the identified issue. If the panel is unable to find a corrective action that will meet the requirements for acceptable risk under SRM, it must prove that the corrective action either increases the safety of the NAS or reduces the safety risk in the NAS. The panel recommends the corrective action. The implementing party continues to work toward identification of a corrective action that meets the SRM requirements and/or continues to work toward managing the risk down to an acceptable level on the implemented change. This applies to existing hazards only. For more information on existing hazards reference Appendix H, *Documenting Existing Hazards Process*. Likewise, if an SRM Panel identifies existing high risk hazards in the NAS, corrective action is necessary. No one is authorized to introduce new high risk as the result of implementing a new change to the NAS.

3.8.5 Causes, System State, and Effect Defined

During the hazard identification phase, the panel identifies and documents potential safety issues, their possible causes, the conditions under which hazards might be realized (system state), and corresponding effects.

Causes are events that result in a hazard or failure, which can occur independently or in combinations. They include, but are not limited to:

a. Human error
b. Latent errors
c. Design flaws
d. Component failure
e. Software errors

A **system state** is defined as the expression of the various conditions, characterized by quantities or qualities in which a system can exist.

It is important to capture the system state that most exposes a hazard. The system description remains within the confines of any operational conditions and assumptions defined in existing documentation. System state can be described using one or some combination of the following terms:

a. **Operational and Procedural** - VFR vs. IFR, Simultaneous Procedures vs. Visual Approach Procedures, etc.
b. **Conditional** - Instrument Meteorological Conditions vs. Visual Meteorological Conditions, peak vs. low traffic, etc.
c. **Physical** - Electromagnetic Environment Effects, precipitation, primary power source vs. back-up power source, closed vs. open runways, dry vs. contaminated runways, etc.

Any given hazard may have a different risk level in a different system state. Hazard assessment must consider all possibilities, from the least to the most likely, allowing for "*worst case*" conditions. It is important to capture all system states to identify worst credible outcomes and unique mitigations. The SRM Panel must ensure that the hazards to be included in the final analysis are "*credible"* hazards considering all applicable existing controls. They can use the following definitions as a guide in making such decisions:

a. **Worst** – The most unfavorable conditions expected (e.g., extremely high levels of traffic, extreme weather disruption)
b. **Credible** – Implies that it is reasonable to expect the assumed combination of extreme conditions will occur within the operational lifetime of the change

The goal of the safety analysis is to define appropriate mitigations for all risks associated with each hazard. While the worst credible outcome may produce the highest risk, the likelihood of the worst credible outcome is often very low. However, a less severe outcome may occur more frequently and result in a higher risk than the worst effect. The mitigations for the two outcomes may be different and both must be identified. It is important for the panel to consider all possible outcomes in order to identify the highest risk and develop effective mitigations for each unique outcome.

The SRM Panel should consider identifying the accumulation of "minor" failures or errors that result in hazards with greater severity or likelihood than would result if the panel considered each failure or error independently.

The **effect** is a description of the potential outcome or harm of the hazard if it occurs in the defined system state.

The Bow-Tie model in Figure 3.8 illustrates the relationship between causes, hazards, and what kind of environment (system state) enables their propagation into the different effects. While it may be used in conducting a safety analysis, the Bow-Tie model is included here as a means to conceptualize safety risk associated with hazards under various conditions. This model assumes each hazard can be represented by one or many causes, having the potential to lead to one or many effects (incidents or events) in various system states.

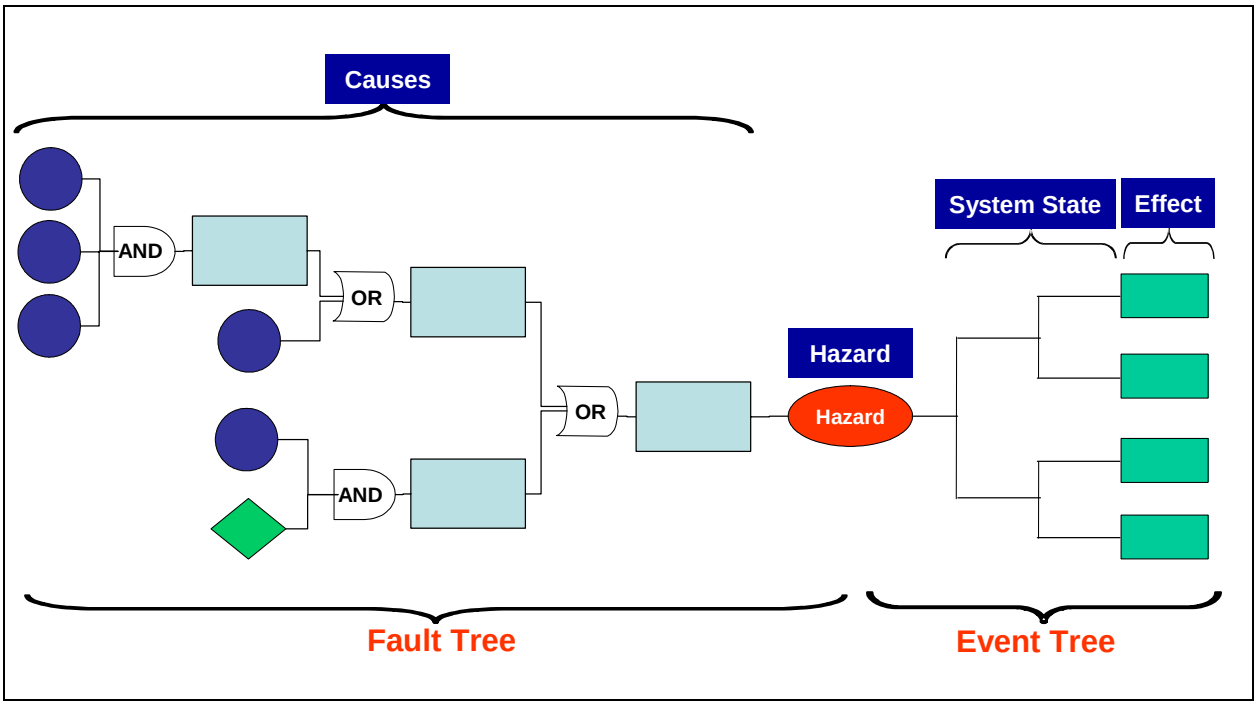


Figure 3.8: The Bow-Tie Model

The Bow-Tie model is a structured approach in which causes of hazards are directly linked to possible outcomes or effects in a single diagram. The underlying analysis can be simple or complex depending on what is appropriate for the change being analyzed.

For each effect associated with the hazard, one assigns a severity. To understand a hazard's severity, one determines the hazard's cause and the circumstances under which it occurred (e.g., the system state). The same model can be used to help determine the likelihoods associated with the different effects that are the result of a particular hazard given the outlined system states. Sections 3.9.1 – 3.9.5, describe severity and likelihood determinations in further detail. Appendix I, *Bow-Tie Model Example*, provides an example of the use of the Bow-Tie model.

3.8.6 Tools and Techniques for Hazard Identification and Analysis

The following tools and techniques can be helpful in identifying and analyzing hazards. In many cases, using a single tool or technique will suffice. However, some cases may require multiple tools and techniques. Service Unit Safety Engineers can provide additional guidance on which tool(s) to use for various types of changes.

Table 3.1 describes a selection of hazard identification and analysis tools and techniques. Appendix G, *Hazard Identification and Analysis Tools and Techniques*, provides more detailed information about the utility and use of tools and techniques. Further information on the tools discussed in Appendix G, *Hazard Identification and Analysis Tools and Techniques,* is available in the FAA AMS Toolset (FAST) and the FAA Human Factors Acquisition Job Aid.

Table 3.1: Selection of Hazard Identification and Analysis Tools and Techniques

Tool or Technique	Summary Description	Page in Appendix G
Preliminary Hazard Analysis (PHA)	The PHA provides an initial overview of the hazards present in the overall flow of the operation. It provides a hazard assessment that is broad, but usually not deep.	G-1
Operational Safety Assessment (OSA)	The OSA is a development tool based on the assessment of hazard severity. It establishes how safety requirements are to be allocated between air and ground components and how performance and interoperability requirements might be influenced.	G-3
Comparative Safety Assessment (CSA)	The CSA provides management with a listing of all of the hazards associated with a change, along with a risk assessment for each alternative hazard combination that is considered. It is used to rank the options for decision-making purposes. The CSA's broad scope is an excellent way to identify issues that may require more detailed hazard identification tools.	G-5
Fault Hazard Analysis (FHA)	The FHA is a deductive method of analysis that personnel can use exclusively as a qualitative analysis or, if desired, can expand to a quantitative one. The FHA requires a detailed investigation of the subsystems to determine component hazard modes, causes of these hazards, and resultant effects on the subsystem and its operation.	G-8
Failure Mode and Effect Analysis (FMEA)	The FMEA determines the results or effects of sub-element failures on a system operation and classifies each potential failure according to its severity.	G-9
Failure Modes, Effects, and Criticality Analysis (FMECA)	The FMECA is an essential function in design from concept through development. To be effective, the FMECA is iterative to correspond with the nature of the design process itself. The FMECA identifies component and sub-system failure modes, including the impact of human error; evaluates the results of the failure modes; determines rates and probability; and demonstrates compliance with safety requirements.	G-9
What-If Analysis	The What-If Analysis methodology identifies hazards, hazardous situations, or specific accident events that could produce an undesirable consequence. One can use the What-If Analysis as a brainstorming method.	G-10
Scenario Analysis	The Scenario Analysis identifies and corrects potentially hazardous situations by postulating accident scenarios in cases where it is credible and physically logical.	G-12
Change Analysis	The Change Analysis analyzes the hazard implications of either planned or incremental changes (e.g., operation, equipment, or procedure).	G-13
Cause-Consequence Analysis	The Cause-Consequence Analysis combines the bottom-up and top-down analysis techniques of Event Trees and Fault Trees. The result is the development of potential complex accident scenarios.	G-15

Tool or Technique	Summary Description	Page in Appendix G
Hazard and Operability Tool (HAZOP)	A group uses the HAZOP to analyze hazards of completely new operations and to review the significance of all of the ways that a process element can malfunction or be incorrectly operated. The technique is essentially a structured brainstorming using specific guide words.	G-17
Interface Analysis	One uses the Interface Analysis to discover the hazardous linkages between interfacing systems.	G-18
Accident/Incident Analysis	The Accident/Incident Analysis uses data on recorded hazardous events. One groups these events in various ways according to a pre-established criterion, usually a common cause or outcome. One then identifies the groupings as hazards.	G-19
Job Safety Analysis (JSA)	One uses this technique to assess in detail the safety considerations in a single job or task..	G-20
Energy Trace and Barrier Analysis (ETBA)	The ETBA is highly structured. It documents all energy sources in system. One identifies the energy sources as hazards. One identifies the barrier between the energy sources and the operators, maintainers, and other systems as mitigations.	G-21
Fault Tree Analysis (FTA)	An FTA is a graphical design technique that can provide an alternative to block diagrams. It is a top-down, deductive approach structured in terms of events. One models faults in terms of failures, anomalies, malfunctions, and human errors.	G-22
Management Oversight and Risk Tree (MORT)	One uses the MORT technique to systematically analyze hazards to examine and determine detailed information about the process and accident contributors.	G-24
Human Error Analysis (HEA)	HEA, in a system context, involves assessing each human-machine interface point, decision, or action for the potential for human error to adversely impact system performance or safety of the system and its users. There are a variety of methodologies for conducting these analyses.	G-26
Job Task Analyses (JTA)	The foundation of the performance of HEA is a task analysis, which describes each human task/sub-task within a system in terms of the perceptual (information intake), cognitive (information processing and decision making), and manual (motor) behaviors required of an operator, maintainer, or support person. It should also identify the skills and information required to complete the tasks; equipment requirements; the task setting; time and accuracy requirements; and the probable human errors and consequences of these errors. There are several tools and techniques for performing task analyses, depending on the level of analysis needed.	G-28

3.8.7 Tool Selection Criteria

Some considerations to take into account when selecting hazard identification/analysis tools include:

a. The necessary information and its availability
b. The timeliness of the necessary information and the amount of time required to conduct the analysis
c. The tool that will provide the appropriate systematic approach to:
   (1.) Identifying the greatest number of relevant hazards
   (2.) Identifying the causes of the hazards
   (3.) Predicting the effects associated with the hazards
   (4.) Assisting in recommending/identifying effective risk mitigations

3.9 Phase 3: Analyze Risk

3.9.1 Analyzing Risk

In this phase, the SRM Panel:

a. Evaluates each hazard (from Phase 2) and the system state in which it potentially exists (from Phases 1 and 2) to determine what controls exist to prevent or reduce the hazard's occurrence or effect(s)
b. Compares a system and/or sub-system, performing its intended function in anticipated operational environments, to those events or conditions that would reduce system operability or service

These events may, if not mitigated, continue until total system degradation and/or failure occurs. These mitigations are called existing controls. Once the SRM Panel documents the existing controls, it estimates the hazard's risk.

An accident rarely results from a single failure or event. Consequently, risk analysis is often not a single binary (on/off, open/close, break/operate) analytical look. While they may result in the simple approach, risk and hazard analyses are also capable of looking into degrees of event analysis or the potential failure resulting from degrading events that may be complex and involve primary, secondary, or even tertiary events.

Risk is defined as the composite of predicted severity and likelihood of the potential effect of a hazard in the worst credible system state. The SRM Panel can use quantitative or qualitative methods to determine the risk, depending on the application and the rigor it uses to analyze and characterize the risk. Different failure modes of the system(s) can impact both severity and likelihood in unique ways.

3.9.2 Existing Controls

In this phase, the SRM Panel evaluates each hazard and the system context in which the hazard potentially exists to determine what prevents or reduces the hazard's occurrence or mitigates its effects. These mitigations are called existing controls. A control can only be considered existing if it has been validated and verified with objective evidence. Until it is validated, it is considered a recommended requirement. Section 3.11.8 further describes validated, verified, and recommended controls.

It is important to document existing controls as the panel's understanding of existing controls impacts its ability to establish credible severity and likelihood determinations. When identifying existing controls, the SRM Panel takes credit for controls specific to the change, hazard, and system state. Table 3.2 provides some examples of existing controls.

Table 3.2: Examples of Existing Controls

Controller	Pilot	Equipment/Technical Operations
• Radar Surveillance − Ground and Airborne • Controller Scanning − Radar − Visual (Out Window) • CA, Minimum Safe Altitude Warning (MSAW), AMASS ASDE-X • Procedures − Specific SOP Reference − FAA Order Reference • Triple Redundant Radio • Controller Intervention • Training − Implementation − Routine Periodic • Management Oversight	• TCAS • Ground Proximity Warning System (GPWS) • Visual Scanning (Out Window) • Radar Surveillance − Airborne • Checklists • Redundancies/Back-up Systems	• Preventative Maintenance • Failure Warnings/Maintenance Alerts • Redundancy Systems − Triple Redundant Radio − Software Redundancy • Diverse Points of Delivery − Microwave and TELCO • Fall Back Systems − Center RADAR Processing (CENRAP) − Direct Access RADAR Channel (DARC) • Software/Hardware Design

3.9.3 Determining Severity

Severity is the measure of how bad the results of an event are predicted to be. One determines severity by the worst credible outcome. The SRM Panel must examine all effects and consider the worst credible severity. One does not consider likelihood when determining severity; determination of severity is independent of likelihood. The goal of the safety analysis is to define appropriate mitigations for all risks associated with each hazard. While the worst credible outcome may produce the highest risk, the likelihood of the worst credible outcome is often very low. However, a less severe outcome may occur more frequently and result in a higher risk than the worst effect. The mitigations for the two outcomes may be different and both must be identified. It is important for the panel to consider all possible outcomes in order to identify the highest risk and develop effective mitigations for each unique outcome.

Table 3.3 provides specific definitions of severity to be used in this phase.

Table 3.3: Severity Definitions

Effect On: ↓	Hazard Severity Classification				
	Minimal **5**	**Minor** **4**	**Major** **3**	**Hazardous** **2**	**Catastrophic** **1**
ATC Services	Conditions resulting in a minimal reduction in ATC services, or a loss of separation resulting in a Category D Runway Incursion (RI)[1], Operational Deviation (OD)[2], or Proximity Event (PE)	Conditions resulting in a slight reduction in ATC services, or a loss of separation resulting in a Category C RI[1] or Operational Error (OE)[2]	Conditions resulting in a partial loss of ATC services, or a loss of separation resulting in a Category B RI[1] or OE[2]	Conditions resulting in a total loss of ATC services, (ATC Zero) or a loss of separation resulting in a Category A RI[1] or OE[2]	Conditions resulting in a collision between aircraft, obstacles or terrain
Flight Crew	– Flightcrew receives TCAS Traffic Advisory (TA) informing of nearby traffic, or, – PD where loss of airborne separation falls within the same parameters of a Category D OE [2] or PE – Minimal effect on operation of aircraft	– Potential for Pilot Deviation (PD) due to TCAS Preventive Resolution Advisory (PRA) advising crew not to deviate from present vertical profile or, – PD where loss of airborne separation falls within the same parameters of Category C (OE) [2] *or* – Reduction of functional capability of aircraft but does not impact overall safety (e.g., normal procedures as per AFM)	– PD due to response to TCAS Corrective Resolution Advisory (CRA) issued advising crew to take vertical action to avoid developing conflict with traffic or, – PD where loss of airborne separation falls within the same parameters of a Category B OE [2] or, – Reduction in safety margin or functional capability of the aircraft, requiring crew to follow abnormal procedures as per AFM	– Near mid-air collision (NMAC) results due to proximity of less than 500 feet from another aircraft or a report is filed by pilot or flight crew member that a collision hazard existed between two or more aircraft – Reduction in safety margin and functional capability of the aircraft requiring crew to follow emergency procedures as per AFM	– Conditions resulting in a mid-air collision (MAC) or impact with obstacle or terrain resulting in hull loss, multiple fatalities, or fatal injury

Effect On: ↓	Hazard Severity Classification				
	Minimal **5**	**Minor** **4**	**Major** **3**	**Hazardous** **2**	**Catastrophic** **1**
Flying Public	– Minimal injury or discomfort to passenger(s)	– Physical discomfort to passenger(s) (e.g., extreme braking action; clear air turbulence causing unexpected movement of aircraft causing injuries to one or two passengers out of their seats) – Minor[3] injury to greater than zero to less or equal to 10% of passengers	– Physical distress on passengers (e.g., abrupt evasive action; severe turbulence causing unexpected aircraft movements) – Minor[3] injury to greater than 10% of passengers	Serious[4] injury to passenger(s)	Fatalities, or fatal[5] injury to passenger(s)

1 – As defined in the 2005 Runway Safety Report
2 – As defined in FAA Order 7210.56, *Air Traffic Quality Assurance*, and Notice JO 7210.663, *Operational Error Reporting, Investigation, and Severity Policies*
3 – Minor Injury - Any injury that is neither fatal nor serious.
4 – Serious Injury - Any injury which: (1) requires hospitalization for more than 48 hours, commencing within 7 days from the date the injury was received; (2) results in a fracture of any bone (except simple fractures of fingers, toes, or nose); (3) causes severe hemorrhages, nerve, muscle, or tendon damage; (4) involves any internal organ; or (5) involves second- or third-degree burns, or any burns affecting more than 5 percent of the body surface.
5 – Fatal Injury - Any injury that results in death within 30 days of the accident.

3.9.4 Likelihood and Risk Assessment

Risk is the composite of predicted severity and likelihood of the potential effect of a hazard in the worst credible system state; likelihood is an expression of how often one expects an event to occur.

One must consider severity in conjunction with the determination of likelihood. Likelihood is determined by how often one can expect the resulting harm to occur at the worst credible severity. Table 3.4 shows likelihood definitions.

The SRM Panel uses NAS Systems likelihood definitions (in the first three columns) when acquiring new or modifying existing systems. AFS uses the Flight Procedures definitions (in the sixth column) when assessing flight procedures. Safety professionals used the likelihood definitions for both NAS Systems and Flight Procedures prior to the development and implementation of the SMS.

The ATO formulated the operational likelihood definitions (in the fourth and fifth columns), which are for use in assessing ATC operations (e.g., airspace changes, ATC procedures and standards) during the development of the SMS.[11] The operational likelihood definitions are based on consideration of the number of aircraft operations and operational hours in the NAS annually; as well as the acceptable level of safety risk, which has been in accepted use within the FAA prior to the SMS and does not constitute a change.

3.9.5 Use of Qualitative and Quantitative Data

In assessing risk, one can use both quantitative and qualitative methods. Using quantitative data is preferred, as it tends to be more objective; however, when quantitative data are not available, it is acceptable to rely on qualitative data and expert judgment. Qualitative judgment varies from person to person, so if only one person is performing the analysis, the result should be considered an opinion. With a team of experts involved in the analysis, one can consider the result qualitative data or expert judgment.

Characteristics of quantitative data include:

a. Data are expressed as a quantity, number, or amount
b. Data tend to be more objective
c. Data allow for more rational analysis and substantiation of findings
d. Modeling

Modeling techniques, such as event tree analysis, permit either statistical or judgmental inputs. If modeling is required and data are available, the risk assessment should be based on statistical or observational data (e.g., radar tracks). Where there is insufficient data to construct purely statistical assessments of risk, judgmental inputs can be used but they should be quantitative. For example, the true rate of a particular type of operation may be unknown, but can be estimated using judgmental input. In all cases, quantitative measures should take into consideration the fact that historical data may not represent future operating environments. In such cases, some adjustment to the input data may be required.

Characteristics of qualitative data include:

[11] Appendix L, *SRM and Operational Changes to the ATC System*, contains information and guidance on applying SRM to operational changes to the ATC system.

a. Data are expressed as a measure of quality
b. Data are subjective
c. Data allow for examination of subjects that can often not be expressed with numbers but by expert judgment

Table 3.4: Likelihood Definitions

	NAS Systems & ATC Operational	NAS Systems		ATC Operational		Flight Procedures
	Quantitative	Qualitative				
		Individual Item/System	ATC Service/ NAS Level System	Per Facility	NAS-wide	
Frequent A	Probability of occurrence per operation/operational hour is equal to or greater than $1x10^{-3}$	Expected to occur about once every 3 months for an item	Continuously experienced in the system	Expected to occur more than once per week	Expected to occur more than every 1-2 days	Probability of occurrence per operation/operational hour is equal to or greater than $1x10^{-5}$
Probable B	Probability of occurrence per operation/operational hour is less than $1x10^{-3}$, but equal to or greater than $1x10^{-5}$	Expected to occur about once per year for an item	Expected to occur frequently in the system	Expected to occur about once every month	Expected to occur about several times per month	
Remote C	Probability of occurrence per operation/operational hour is less than or equal to $1x10^{-5}$ but equal to or greater than $1x10^{-7}$	Expected to occur several times in the life cycle of an item	Expected to occur numerous times in system life cycle	Expected to occur about once every year	Expected to occur about once every few months	Probability of occurrence per operation/operational hour is less than or equal to $1x10^{-5}$ but equal to or greater than $1x10^{-7}$
Extremely Remote D	Probability of occurrence per operation/operational hour is less than or equal to $1x10^{-7}$ but equal to or greater than $1x10^{-9}$	Unlikely to occur, but possible in an item's life cycle	Expected to occur several times in the system life cycle	Expected to occur about once every 10-100 years	Expected to occur about once every 3 years	Probability of occurrence per operation/operational hour is less than or equal to $1x10^{-7}$ but equal to or greater than $1x10^{-9}$
Extremely Improbable E	Probability of occurrence per operation/operational hour is less than $1x10^{-9}$	So unlikely that it can be assumed that it will not occur in an item's life cycle	Unlikely to occur, but possible in system life cycle	Expected to occur less than once every 100 years	Expected to occur less than once every 30 years	Probability of occurrence per operation/operational hour is less than $1x10^{-9}$

3.10 Phase 4: Assess Risk

3.10.1 Assessing Risk

In this phase, the SRM Panel:

a. Compares each hazard's associated risk (as identified in Phase 3) and plots the risks on a pre-planned risk acceptability matrix
b. Determines a hazard's priority by the location of its associated safety risk on this risk matrix
c. Gives higher priority hazards the greatest attention in the treatment of risk

3.10.2 Risk Matrix Definition

A risk matrix is a graphical means of determining risk levels. The rows in the matrix reflect previously introduced severity categories, and its columns reflect previously introduced likelihood categories. The SRM Panel assesses risk by using the risk matrix in Figure 3.9.

The risk levels used in the matrix are defined as:

a. **High** – unacceptable risk; change cannot be implemented unless the hazard's associated risk is mitigated so that risk is reduced to a medium or low level. Tracking, monitoring, and management are required. Hazards with catastrophic effects that are caused by: (1) single point events or failures, (2) common cause events or failures, or (3) undetectable latent events in combination with single point or common cause events, are considered high risk, even if the possibility of occurrence is extremely improbable.
b. **Medium** – acceptable risk; minimum acceptable safety objective; change may be implemented, but tracking, monitoring, and management are required.
c. **Low** – acceptable without restriction or limitation; hazards are not required to be actively managed but must be documented.

A catastrophic severity and corresponding extremely improbable likelihood qualify as medium risk, as long as the effect is not the result of a single point or common cause failure. If the cause is a single point or common cause failure, the effect of the hazard is categorized as high risk and placed in the red part of the split cell in the bottom right corner of the matrix.

A **single point failure** is defined as a failure of an item that would result in the failure of the system and is not compensated for by redundancy or an alternative operational procedure. An example of a single point failure is a system with redundant hardware, in which both pieces of hardware rely on the same battery for power. In this case, if the battery fails, the system will fail.

A **common cause failure** is defined as a single fault resulting in the corresponding failure of multiple components. An example of a common cause failure is redundant computers running on the same software, which is susceptible to the same software bugs.

Severity / Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A					
Probable B					
Remote C					
Extremely Remote D					
Extremely Improbable E					*

* Unacceptable with Single Point and/or Common Cause Failures

High Risk
Medium Risk
Low Risk

Figure 3.9: Risk Matrix[12]

3.10.3 Types of Risk

a. **Initial risk** is the composite of the severity and likelihood of a hazard considering only verified controls and documented assumptions for a given system state. It describes the risk at the preliminary or beginning stage of a proposed change, program or assessment.
b. **Current risk** is the predicted severity and likelihood of a hazard at the current time. When determining current risk, both validated controls and verified controls may be used in the risk assessment. Current risk may change based on the actions taken by the decision-maker that relate to the validation and/or verification of the controls associated with a hazard.
c. **Predicted residual risk** is the term used until the safety analysis is complete and all safety requirements have been verified. Predicted residual risk is based on the assumption that all safety requirements will be validated and verified.
d. **Residual risk** is the risk that remains after all control techniques have been implemented or exhausted and all controls have been verified. Only verified controls can be used to assess residual risk.

[12] As specified in FAA Order 1100.161, *Air Traffic Safety Oversight*, Chapter 4.1.b, "In the case where the hazard and/or failure of the system has a direct impact on aircraft operations, ATO may evaluate those systems in accordance with the risk chart and classification documented in Advisory Circular (AC) 25.1309-1A, System and Design Analysis, current edition; International Civil Aviation Organization (ICAO) Standards and Recommended Practices (SARP); and National Standards and Operations Specification. For example, hazards associated with an Instrument Landing System (ILS), a ground system (ILS outputs have a direct effect on the aircraft) would be classified, for risk, according to AC 25.1309-1A. Other examples include navigational aids (NAVAID) and Microwave Landing Systems (MLS)."

3.10.4 Ranking and Prioritizing Risk for Each Hazard

The SRM Panel follows these guidelines in ranking and prioritizing risk for each hazard:

a. Rank hazards according to the severity and the likelihood of their associated risk (illustrated by where they fall on the risk matrix).
b. To plot a hazard on the risk matrix, select the appropriate severity column (based on the severity definitions in Table 3.3) and move down to the appropriate likelihood row (based on the likelihood definitions in Table 3.4).
c. Plot the hazard in the box where the severity and likelihood of the effect associated with the hazard meet.
d. If this box is red, the risk associated with the hazard is high; if the box is yellow, the risk associated with the hazard is medium; and if the box is green, the risk associated with the hazard is low.

Ranking the risks associated with the identified hazards prioritizes treatment and mitigation. High risk outcomes must be mitigated before the proposed change can be implemented.

3.10.5 Handling High Risk Hazards

When a High Risk Hazard (HRH) is identified by an SRM Panel or change proponent, the proposed change cannot be implemented until the following conditions have been met:

a. The HRH is mitigated to an acceptable level of risk (medium or low)
b. The risk is accepted
c. The mitigations are approved by AOV

For specific guidance regarding the AOV HRH concurrence/approval process and modeling requirements, reference FAA Order 8000.365, *Safety Oversight Circulars (SOC);* AOV SOC 07-02, *AOV Concurrence/Approval at Various Phases of Safety Risk Management Documentation and Mitigations for Initial High-Risk Hazards;* and AOV SOC 07-05, *AOV Guidance on Safety Risk Modeling of High Risk Hazards.*

3.11 Phase 5: Treat Risk

3.11.1 Treating Risk

In this phase, the SRM Panel develops and manages options to deal with risk (from Phase 4). Effectively treating risk involves:

a. Identifying feasible mitigation options
b. Developing a risk treatment plan accepting the predicted residual risk
c. Developing a monitoring plan detailing review cycles for evaluating the effectiveness of mitigations
d. Implementing and verifying the mitigations
e. Monitoring the effectiveness of the mitigation

In the treat risk phase, the SRM Panel develops alternative strategies for managing the risk associated with a hazard. These strategies become actions that reduce the risk of the hazard's effects on the system (e.g., human interface, operation, equipment, procedures). While the SRM Panel develops options to mitigate risk, it is the responsibility of the organization(s) making the NAS change to implement and verify the mitigations, as well as monitor their effectiveness.

3.11.2 Risk Mitigation Definition

Risk mitigation is taking action to reduce the risk of the hazard's effects. Examples of risk mitigation include:

a. Revising the system design
b. Modifying operational procedures
c. Establishing contingency arrangements

When risk is determined to be unacceptable, the SRM Panel identifies and evaluates risk mitigation measures that would reduce the risk to an acceptable level. Once identified, the SRM Panel assesses how the proposed mitigation measures affect the overall risk. If necessary, the team repeats the process until a combination of measures reduce the risk to an acceptable level.

When risk mitigation strategies cross organizations, those stakeholder organizations must approve documentation and accept risk in accordance with Table 3.7 in Section 3.13.1 and Table 3.8 in Section 3.14.3.

If the risk does not meet the pre-determined acceptability criteria, it must always be reduced to a level that is acceptable, using appropriate mitigation procedures to implement the change. Even when the risk is classified as acceptable, if any measures could further reduce the risk, the appropriate party should:

a. Make an effort to implement these measures, if feasible
b. Consider the technical feasibility of further reducing the risk
c. Evaluate all such cases individually

Remember that when an individual or organization "accepts" a risk, it does not mean that the risk is eliminated. Some level of risk remains; however, the individual or organization has accepted that the predicted residual risk is sufficiently low such that it is outweighed by the benefits.

If SRM Panel members identify systemic hazards, then the impacted managers identify and implement risk mitigation efforts. Managers should also assess proposed mitigations for possible collateral system impacts and initiate appropriate corrective actions.

3.11.3 Risk Mitigation Strategies

Risk mitigation requires management's informed decision to approve, fund, schedule, and implement one or more risk mitigation strategies. The objective of this phase is to implement appropriate plans to mitigate the risk associated with identified hazards and their effects. The SRM Panel develops, documents, and recommends appropriate risk mitigation strategies. The risk mitigation approach selected may fall into one or more of the following categories:

a. Risk avoidance strategy
b. Risk transfer strategy
c. Risk assumption strategy
d. Risk control strategy

Once the SRM Panel selects and develops risk mitigation strategies, management can identify the impact on other organization(s) and coordinate/obtain agreement on those strategies with the affected organization(s). In addition, the SRM Panel establishes a monitoring plan to ensure

that risk mitigation strategies are effective. It repeats the risk mitigation process until risk is reduced to an acceptable level.

Hazard tracking is a key element of this risk management phase. Section 3.11.11 provides further detail on hazard tracking.

3.11.4 Risk Avoidance Strategy

The risk avoidance strategy averts the potential of occurrence and/or consequence by selecting a different approach or by not participating in the operation, procedure, or system (hardware and software) development. SRM Panels may pursue this technique when multiple alternatives or options are available.

The risk avoidance strategy is more likely used as the basis for a “go” or “no-go” decision at the start of an operation or program. The avoidance of risk is from the perspective of the overall organization. Thus, an avoidance strategy is one that involves all the stakeholders associated with the proposed change.

3.11.5 Risk Transfer Strategy

The risk transfer strategy shifts the ownership of risk to another party. Organizations transfer risk primarily to assign ownership to the organization or operation most capable of managing it. The receiving party must accept the risk, which must be documented (e.g., Letter of Agreement, Statement of Agreement, Memorandum of Agreement).

Examples of risk transfer may include:

a. Transfer of aircraft separation responsibility in applying visual separation from the air traffic controller to the pilot
b. Development of new policies or procedures to change ownership of a NAS element to a more appropriate organization
c. Contract procurement for specialized tasks from more appropriate sources (e.g., contract maintenance)
d. Transfer of ATC systems from the acquisition organization to the organization that provides maintenance

The receiving organization may be better equipped to mitigate the risk at the operational or organizational level. Transfer of risk, while theoretically an acceptable means of mitigating risk, cannot be the only method used to treat high risk associated with a hazard. The SRM Panel must still mitigate the safety risk to medium or low before it can be accepted in the NAS.

In addition, when hazards (and associated risks) that are outside the scope of the ATO SMS are identified (e.g., OSHA, physical, and information security), organizations transfer the management and mitigation of these risks to the appropriate organization.

3.11.6 Risk Assumption Strategy

The risk assumption strategy is simply accepting the likelihood or probability and the consequences associated with a risk’s occurrence. It is not acceptable to use an assumption strategy to treat high risk associated with a hazard. The safety risk must still be reduced to medium or low before it can be accepted into the NAS, as required by SRM documented in this manual.

3.11.7 Risk Control Strategy

A **control** is anything that mitigates the risk of a hazard's effects. A control is the same as a safety requirement. All controls must be written in requirement language.

A risk control strategy helps to develop options and alternatives and take actions that lower or eliminate the risk. Examples include implementing additional policies or procedures, developing redundant systems and/or components, and using alternate sources of production. When this is done, it becomes a safety requirement. A correct requirement is unambiguous and verifiable. Controls can be complex or simple.

3.11.8 Status of a Control

There are three types of controls:

a. **Validated** – Those controls and requirements that are unambiguous, correct, complete, and verifiable
b. **Verified** – Those controls and requirements that are objectively determined to have been met by the design solution
c. **Recommended** – Those controls that have the potential to mitigate a hazard or risk, but have not yet been verified as part of the system or its requirements

In the engineering environment, controls are usually validated and verified before the change is implemented. In the procedures/operations environment, controls are validated before the change is approved, and then verified through the continuous monitoring process. The expected time needed to verify a control may vary. If the hazard occurs at a higher frequency than identified in the safety assessment, then the safety requirement may not be valid and will need to be reevaluated. Once the target level of risk has been achieved, it will be monitored through existing NAS monitoring processes, such as facility or procedure evaluations to ensure that the target level of risk has been reached and maintained.

3.11.9 Safety Order of Precedence

There is a preferred order for the development of risk mitigation controls:

a. Design for minimum risk
b. Incorporate safety devices
c. Provide warning
d. Develop procedures and training

Safety professionals use these in relation to system (hardware/software) development and modification. Table 3.5 shows the safety order of precedence, which reflects this order.

Table 3.5: Safety Order of Precedence

Description	Priority	Definition	Example
Design for minimum risk	1	Design the system (e.g., operation, procedure, human-to-system interface, or equipment) to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level by selecting alternatives.	1. If a collision hazard exists because of a transition to a higher Minimum En Route Altitude at a crossing point, moving the crossing point to another location would eliminate the risk. 2. If "loss of power" is a hazard to a system, adding a second independent power source reduces the likelihood of the "loss of power" hazard.
Incorporate safety devices	2	If identified risks cannot be eliminated through alternative selection, reduce the risk by using fixed, automatic, or other safety features or devices and make provisions for periodic functional checks of safety devices.	1. An automatic "low altitude" detector in a surveillance system 2. Interlocks to prevent exposure to radiation or high voltage 3. Automatic engine restart logic
Provide warning	3	When neither alternatives nor safety devices can effectively eliminate or adequately reduce risk, warning devices or procedures are used to detect the condition and to produce an adequate warning. The warning must be provided in time to avert the hazard's effects. Warnings and their application are designed to minimize the likelihood of inappropriate human reaction and response.	1. A warning displayed on an operator's panel 2. "Engine Failure" light in a helicopter 3. Flashing Minimum Safe Altitude Warning or Conflict Alert Indicator on a radar screen
Develop procedures and training	4	Where it is impractical to eliminate risks through alternative selection, safety features, and warning devices, procedures and training are used. However, management must concur when procedures and training are solely applied to reduce risks of catastrophic or hazardous severity.	1. A missed approach procedure 2. Training in stall/spin recovery 3. Procedure to vector an aircraft above a Minimum Safe Altitude on a Very High Frequency Omni-directional Range airway 4. Procedures for loss of communications

3.11.10 Risk Not Sufficiently Reduced

If the risk cannot be reduced to an acceptable level after attempting all possible mitigation measures, then the change does not satisfy the safety requirements. Therefore, the change proponent must either revise the original objectives or abandon the proposed change. If the proposal is unacceptable, the change cannot be implemented. This conclusion must be included in the SRMD.

3.11.11 Hazard Tracking

Hazard tracking is a dynamic process in which hazards and their associated safety risk information and safety requirements are entered into a database. The information is updated throughout the lifecycle of a system or change. Hazard tracking, in part, includes documenting safety requirements, providing the status of requirements validation and verification, verifying implementation, and updating the current and predicted residual risk levels before acceptance. Hazard tracking also assesses the effectiveness of existing and recommended safety requirements in the control of the identified hazards. The purpose of hazard tracking and risk resolution is to ensure a closed-loop process of managing safety hazards and risks.

The ATO uses a restricted access, web-based system to document all hazards and their associated risk information. All Service Units are required to use a hazard tracking system provided by the ATO to capture all safety hazards. The ATO requires that organizations formally identify all hazards, and track and monitor all initial medium and high risk hazards for the lifecycle of the system or change, or until they mitigate the risk to low (as defined in Section 3.10.2). Organizations must also verify the effectiveness of the controls mitigating all risks through continuous monitoring. If through SRM processes and/or safety assurance measures the mitigations are found ineffective in reducing the risk to an acceptable level, the change proponent and/or SRM Panel must reassess the risk and implement additional mitigations until further monitoring illustrates the risk is mitigated to low. Hazards with low associated risk by definition meet ATO safety requirements for target level and may not require further mitigation.

The ATO's hazard tracking system allows SRM practitioners to enter hazard and mitigation data via the use of various forms including the PHA, PHL, Safety Requirements Verification Table (SRVT), Safety Action Record (SAR), System Hazard Analysis, Sub-system Hazard Analysis, and the Operating and Support Hazard Analysis.

A key principle of the SMS is that SRM and safety assurance are integrated. Through the SRM process, the ATO develops safety risk mitigations and monitoring plans. Through safety assurance processes, the ATO monitors those mitigations and identifies new hazards or necessary NAS changes, which must go through the SRM process. Hazard tracking is a means to ensure that these two SMS components function together to manage safety risk.

3.11.12 Training and Access to HTS

Currently, the ATO uses the Hazard Tracking System (HTS) to track hazards. It is a secure web site housed behind the FAA's firewall. There are two separate HTS interfaces—one for systems acquisitions/engineering and one for operations. ATO employees can obtain access to, or training on, the system by contacting their Service Unit's Safety Manager or Safety Engineer.

3.11.13 Developing a Control Implementation/Monitoring Plan

In addition to tracking the hazards, the SRM Panel develops a plan to:

a. Verify the risk mitigations
b. Monitor the effectiveness of those mitigations
c. Conduct the post-implementation assessments to verify the results of the analysis

These actions are part of the treat risk phase of the safety analysis. A sample Recommended Control Implementation/Monitoring Plan is shown in Table 3.6.

Table 3.6: Sample Recommended Control Implementation/Monitoring Plan

Task	Responsible	Due Date/ Frequency	Status
Implementation of Controls			
The recommended mitigation that was designed for the change	Individual, division, or organization required to render account concerning the identified task	The date by which the responsible party must have completed the identified task	The state of the task
Example: Safety device X will be installed in Equipment Z.	Example: ZDC Technicians	Example: December 5, 2010	Example: Open*
Monitoring			
A function to be performed; an objective	Individual, division, or organization required to render account concerning the identified task	The frequency that the task will be performed	The state of the task
Example: Internal audit of the maintenance records	Example: Quality Assurance Office	Example: Monthly, quarterly, etc.	Example: Ongoing*, Closed

* "Open" meaning that the due date of the task has not arrived; "Closed" meaning that the task has been completed (generally one would want to include the date of task completion). Sometimes the task is considered to be "Ongoing", meaning that the task is to be performed throughout the lifecycle of the system.

The ATO requires that employees formally monitor all initial medium and high risk hazards for the lifecycle of the system or change, or until they mitigate the risk to low (as defined in Section 3. 10.2) and verify the effectiveness of the controls mitigating the risk. After mitigations have been verified through monitoring and a target level of risk has been achieved, the change proponent can continue current/existing monitoring and evaluation processes, such that the change becomes the standard operation procedure.

Safety professionals conduct post-implementation assessments for the life of the system or change, as defined in the SRMD monitoring plan. The frequency of assessments depends on the type, the potential safety impact, and/or the complexity of the change, as well as the depth and breadth of the original analysis. Inclusive in these assessments is updating the SRMD; existing support mechanisms should be considered. These support mechanisms may include IOT&E, Flight Inspection, the Air Traffic Evaluation and Auditing Program, NASTEP, and SRM audits.

3.12 SRMD

3.12.1 SRMD: Tool for Decision Making

An SRMD thoroughly describes the safety analysis for a proposed change. It documents the evidence to support whether the proposed change to the system is acceptable from a safety risk perspective. The SRMD also contributes (from a programmatic or management perspective) to the decision to implement a change. The Service Unit responsible for implementing the change maintains all documentation associated with the SRM process, including the SRMD, for the lifecycle of the system or change.

The SRMD is a living document that may be modified during the lifecycle of the program. Section 3.13.9 discusses this further.

3.12.2 SRMD Contents

An SRMD provides sufficient detail about a proposed change to a current system or the introduction of a completely new system into the NAS. It should be a single source that enables the management official to understand the change, its associated risks, and corrective steps taken (or proposed) to reduce the initial and subsequent residual risks to an acceptable level. The document must stand alone (i.e., it must contain sufficient detail about the current or proposed system to enable the reader to comprehend what steps have been taken to identify safety issues and the corrective steps taken (or proposed)).

An SRMD contains, at a minimum:

a. Identification of the system to be introduced or changed, including:
   (1.) A description of the current system and proposed change or introduction
   (2.) Current controls in place
   (3.) Pertinent interfaces and support systems required by the introduction and/or change to function properly
   (4.) Reference to any SRMDs submitted on the current system or changes being analyzed
   (5.) A statement reflecting the impact of the change or introduction (local, regional, national, etc.)
b. Identification of hazards and causal factors
   (1.) Description of methodology and tools used
   (2.) Existing controls affected by the introduction and/or change proposed
   (3.) The hazards and scenarios and/or circumstances where they exist
c. Analysis, assessment, and mitigation of the associated risks
   (1.) Documentation of the identified risks including: Initial risk level (in terms of severity and likelihood), when and how they appear in the current or proposed system
   If associated with existing risks and/or controls, and how the introduction of a new system or change in the existing system affects the risk
   (2.) Controls (mitigations) and their effect on identified risks
   (3.) Predicted residual and accepted risks
   (4.) Documentation of how the risks and their associated controls will be tracked and monitored throughout the lifecycle of the system or change
d. Strategy for validation and verification of the proposed change or introduction
   (1.) Means that will be used to obtain measurable data to monitor the effectiveness of the control
      (a.) Who will be responsible for reporting, collecting, and analyzing the data
      (b.) How the data will be analyzed
   (2.) Means that will be used to determine if adjoining systems are adversely affected
      (a.) Who will be responsible for reporting, collecting, and analyzing the data
      (b.) How will the data be analyzed
   (3.) What will determine that safety requirements (existing and recommended) are met and satisfied
   (4.) Future plans for updating the present SRMD

The SRM Panel documents any change that could have safety consequences in the provision of ATC and navigation services. The scale of an SRMD varies depending on the type and complexity of a proposed system change.

The level (i.e., national, Service Area, or local) at which SRM is initiated may vary by organization or change proponent. If the change is at the Service Area or local levels, two methods for documenting SRM can be used:

a. Address the change in a system-wide SRMD through site-specific parameter ranges
b. Develop and append a local-level SRMD to the larger, system-wide SRMD

While panels strive to reach consensus, there may be instances in which not all panel members agree on the results of the safety analysis. In that case, the results are documented, ensuring that the opinions of dissenters are also captured and delivered to the decision-maker.

Appendix J, *High-level SRMD Guidance*, contains guidance on required SRMD information. Appendix K, *SRMD Template*, provides a format example that should be tailored to the specific proposed change and corresponding documentation needs. Appendix L, *SRMD Review Checklist*, contains criteria by which SRM Panels can evaluate the completeness of an SRMD. The SRMD should be written to be understood by a reviewer familiar with the discipline(s) relevant to the change (e.g., terminal controller, center controller, Navigation/Communication, Radar Technical Operations Specialist). There should be enough detail that a reviewer unfamiliar with the program, project, or facility can understand the change and the system within which it is contained. The SRMD should include thorough descriptions of the identified hazards and provide rationales for the panel's severity and likelihood assessments for each hazard. Utilizing the SRMD Review Checklist for quality control will minimize delays caused by clarifications requested by SRMD reviewers and approvers.

Specific guidance for certain types of changes (e.g., waivers) can be found in FAA Order 1800.66, *Configuration Management Policy*; FAA Order 1800.6, *Unsatisfactory Condition Report (UCR)*; and FAA Order JO 1800.3, *NAS Change Proposal (NCP) Process Support of the Safety Management System*. In addition, the latest guidance packages are located in the SMS Directorate portion of the ATO Experience web site (http://atoexperience.faa.gov/safety).

The originating facility/organization assigns SRM documentation numbering when drafting the document. Figure 3.10 depicts SRMD naming conventions for both acquisition and operations changes.

Not all qualifiers will apply to every change; the facility/organization uses each type only when applicable. The Life Cycle Phase numbering only applies to acquisition changes. Examples include:

a. Acquisitions: SRMD-SU-Program/Project name-Analysis Type-YYYY-XXX
b. Analysis Type: SRMD-ATO-E-ERAM-SSHA-2007-001
c. NCP: SRMD-ATO-E-ERAM-NCP Surveillance Processor-2007-001
d. DCP: SRMD-ATO-E-ERAM-DCP- 7110.65-2007-001
e. Waiver: SRMD-ATO-E-OSH-2007-001
f. Legacy Systems: NCP Change to NAS
   (1.) SRMD-ATO-T-WAAS-SW upgrade1-2007-001
   (2.) SRMD-ATO-T-WAAS-SW upgrade2-2007-002
g. Legacy Systems: DCP Change to NAS
   (1.) SRMD-ATO-E-WAAS-DCP- Change2 Title -2007-002
h. Stand Alone Change to NAS for Operation, Procedure, or Technical:
   (1.) SRMD-ATO-E- RNP-SAAAR-2007-010

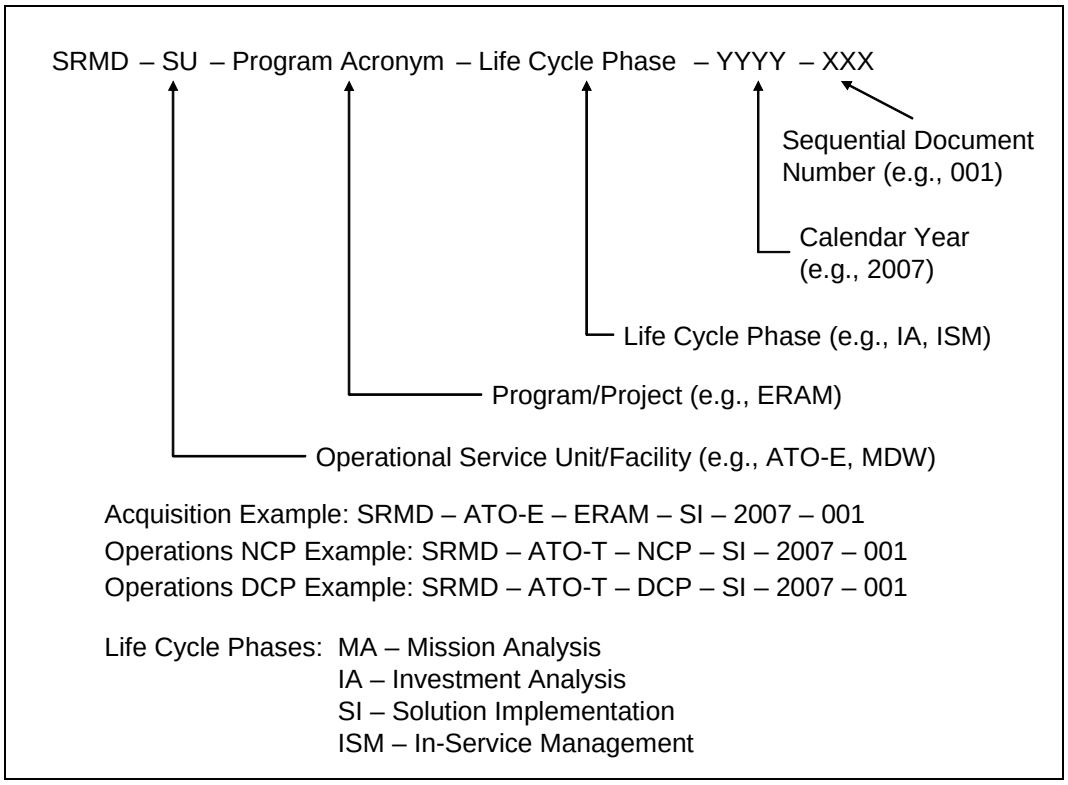


Figure 3.10: SRMD Naming Convention

3.12.3 Additional Resources for SRMD Development

In many instances, existing acquisition and system engineering processes produce documents that SRM Panels use to support the analysis portion of an SRMD. In particular, FAST includes SRMGSA documentation and templates for each stage of the AMS lifecycle. Appendix N, *Deployment Planning Process with SRM,* discusses the relationship between SRM and the Deployment Planning Process.

Many of the FAA and ATO handbooks address safety aspects of specialty engineering; in addition, many of the current system safety engineering processes produce documents compatible with the objectives or elements of an SRMD (e.g., OSA, CSA, System Safety Assessment Report (SSAR)).

3.12.4 SRMD Benefits

An SRMD provides a standardized approach to developing a safety case that:

a. Reduces omissions and inconsistencies in safety analysis preparation and conduct
b. Eases documentation development
c. Makes the sharing of safety risk data more manageable
d. Strengthens SRM skills
e. Encourages a safety culture
f. Ensures operational safety data are monitored to reduce hazards
g. Provides assurance to decision-makers that SMS processes are being followed
h. Establishes responsibility/accountability
i. Makes the process repeatable and reduces re-study of similar change proposals

3.12.5 Difference Between Risk Acceptance and SRMD Approval

Approving the SRMD means that the approving party (see Section 3.13.1 and Table 3.7) agrees that the analysis accurately reflects the safety risk associated with the change, the underlying assumptions are correct, and the findings are complete and accurate.

Accepting the safety risk is a certification by the appropriate management official that he/she understands the safety risk associated with the change and he/she accepts that safety risk.

Both approving the SRMD and accepting the safety risk are necessary, along with other inputs (e.g., costs, benefits), before implementing a change in the NAS.

3.13 SRMD Approvals

3.13.1 SRMD Approval Level Requirements

SRMD approvals depend on the span of the program, its associated risk(s), the mitigation(s) used to control the risk, and other Service Unit specific guidance. **SRM Documentation Approval** is certification that the documentation was developed properly, hazards were systematically identified, risk was appropriately assigned, suitable mitigations were proposed, and a sound implementation and monitoring plan was prepared. SRMD approval *does not* constitute acceptance of the risk associated with the change or approval to implement the change.

The approval and review of an SRMD follows a process for establishing and maintaining quality assurance for the review and evaluation of ATO SRM documentation. The SRM Panel should involve the approving authority early in the SRM process to obtain agreement on the assumptions and processes that it will use, particularly if AOV SOC 07-02, *AOV Concurrence/ Approval at Various Phases of Safety Risk Management Documentation and Mitigations for Initial High Risk Hazards*, and AOV SOC 07-05, *AOV Guidance on Safety Risk Modeling of High-Risk Hazards*, are being followed. Table 3.7 depicts the level of approval required for an SRMD based on the nature of the change and the risk identified.

Table 3.7: SRMD Approval Level Requirements

SRMD Approval Level Required		
Service Unit	**Safety Services**	**AOV**
• For SRMDS that identify medium or low initial safety risk, where the safety risk and controls/mitigations: – stay within the ATO Service Unit, the SRMD is approved within the Service Unit per Service Unit guidance – span ATO Service Units, the SRMD is approved within each affected Service Unit per each Service Unit's guidance – involve LOBs outside of ATO (e.g., ARP or AVS), the SRMD is approved by each affected LOB per each LOB's guidance • Any SRMD that requires Safety Services' approval	Any SRMD that: • Involves changes that require AOV approval • Has identified high initial safety risk • Involves changes to, or replacement of, a system that if lost or malfunctioning would require application of contingency procedures involving increased separation standards or would result in "ATC Zero" status (e.g., ATOP or C-ARTS) • Involves changes in the periodicity of maintenance or inspection (including flight inspection) of systems described above (in 3rd bullet)	Not Applicable - Do not approve SRMDs (see Section 3.13.6)

3.13.2 Service Unit SRMD Approval

The first column in Table 3.7 depicts the instances when the Service Unit will be involved in SRMD approval. If the SRMD is to be approved at a high level within the Service Unit (certainly at the Vice President level, but possibly below), then the Safety Manager must first approve the SRMD before it is submitted to the Director or Vice President. If the SRMD is sent outside the Service Unit for approval (to another operational Service Unit, LOB, Safety Services, or AOV), the Safety Manager approves the SRMD before it leaves the Service Unit.

Service Units may develop additional Service Unit-specific guidance specifying when the Service Unit's Safety Manager and Safety Engineer must be involved in the SRM process and documentation approval requirements. In addition, the Safety Manager and/or Safety Engineer must be available to provide input to the management official(s) who will accept the risk associated with the change.

3.13.3 Safety Services SRMD Approval

The second column of Table 3.7 summarizes the circumstances under which Safety Services approves SRMDs. Safety Services' SRMD approval is a technical and non-technical assessment by subject matter experts to verify that the SRM process has been followed, the safety documentation is complete, and it adheres to the SMS Manual principles and guidelines. The ATO SSWG reviews SRMDs related to system acquisition changes and the SOWG reviews SRMDs related to operational changes.

3.13.4 ATO SSWG

The ATO SSWG is a technically qualified advisory group sponsored by the Safety Services SMS Directorate and consists of FAA system safety professionals from the Service Units and other LOBs (as required). The purpose of the SSWG is to provide system acquisition guidance for conducting SRM in accordance with this manual and the SRMGSA. The SSWG is responsible for advising the Director of SMS regarding reviews of Program Safety Plans and SRMDs, including safety analyses as appropriate to the nature of the proposed change. In addition, the SSWG advises the Service Units and LOBs in establishing system safety and SRM programs for system acquisitions and changes to legacy systems.

3.13.5 ATO SOWG

The ATO SOWG is a technically qualified operational advisory group sponsored by the Safety Services SMS Directorate and made up of FAA safety professionals from the Service Units, ATO Safety Offices, and other LOBs (as required). The purpose of the SOWG is to provide guidance for conducting SRM in accordance with this manual, ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*, FAA Order 1100.161, *Air Traffic Safety Oversight*, and various AOV SOCs. As requested by the Service Units, the SOWG will review preliminary safety documentation for proposed SRMDs in accordance with SOC 07-02, *AOV Concurrence/Approval at Various Phases of Safety Risk Management Documentation and Mitigations for Initial High-Risk Hazards* and SOC 07-05, *AOV Guidance on Safety Risk Modeling of High Risk Hazards*.

3.13.6 AOV Approvals

As depicted in the third column of Table 3.7, AOV *does not* approve SRMDs. For those items that do require AOV approval and AOV acceptance, refer to Sections 3.4.4 - 3.4.6.

3.13.7 Post SRMD Approval

The change proponent retains a copy of the SRMD for the lifecycle of the system or change. Upon request, the proponent of the change provides Safety Services with copies of SRMDs.

SRMDs may also serve as inputs to existing approval processes (e.g., the NAS Change Proposal (NCP) process, Document Change Proposal process, AMS processes/milestones).

3.13.8 SRMDs Related to Changes Not Approved or Implemented

The SRMD is kept on file even if it is not approved or if the change is not implemented. ATO employees can use this information in assessing similar change proposals or as inputs to SRMDs for other change proposals. SRMDs that are not approved, or those used by a decision-maker in his/her decision not to implement a change, also provide proof that the SMS is performing its intended function (i.e., reducing the safety risk in the NAS). Safety Services and/or AOV may also audit this documentation.

3.13.9 SRMD Lifecycle

The results of safety analyses are a part of the system baseline information. ATO employees may need to update or change an SRMD as a project progresses and as they modify decisions. Safety monitoring may indicate that the controls are less effective than originally expected or that additional hazards exist, which may require additional mitigations. Any change that may affect the assumptions or hazards identified in the SRMD or the estimated risk necessitates an amendment to the SRMD.

In addition, the SRMD includes a monitoring plan to conduct post-implementation assessments to verify the results of the previous analyses and update the SRMD. While necessary for the life of the system or change, the periodicity of these assessments may vary depending on the type, potential safety impact, and/or complexity of the change, as well as the depth and breadth of the original analysis.

When developing the plans to monitor the change and update the SRMD, existing support mechanisms should be taken into account. These include IOT&E, Flight Inspection, the Air Traffic Evaluation and Auditing Program, NASTEP, and Safety Services SRM audits. Based on the results of audits and evaluations of how the system performs, an organization may need to modify the SRMD, which could include reopening the safety analysis for additional assessment. Chapter 4, *Safety Assurance*, further describes these processes.

3.14 Accepting Risk

3.14.1 Effect of SRM on Safety Levels

Through SRM, decision-makers knowingly accept risk into the NAS and thus are better able to manage it; this leads to increased safety. Understanding the consequences of risk increases the ability to anticipate and control the impacts of internal and/or external events on a program.

3.14.2 Accepting Safety Risk

Risk Acceptance is the certification by the appropriate management official that he/she understands the safety risk associated with the change, the mitigations are feasible and will be implemented, and he/she accepts that safety risk into the NAS.

Accepting the safety risk is a prerequisite to making a proposed change. Risk acceptance is based on predicted residual risk. Accepting the safety risk is different from approving an SRMD.

Approving an SRMD indicates that the analysis accurately reflects the safety risk associated with the change, the underlying assumptions are correct, and the findings are complete and accurate.

3.14.3 Authority to Accept Safety Risk

The acceptance of the safety risk depends on the span of the program or change, its associated risk, and the mitigation used to control the risk. Only those responsible for the change and in a position to manage the risk can accept the risk into the NAS.

Changes that have high initial safety risk, but have been mitigated to medium or low, in which safety risk and/or controls/mitigations:

a. Stay within the Service Unit; the Service Unit Vice President accepts the safety risk
b. Span Service Units; each affected Service Unit's Vice President accepts the safety risk
c. Go to an LOB outside of the ATO (e.g., to ARP and/or AVS); the Service Unit Vice President and the heads of each affected LOB accept the safety risk

Changes with medium or low initial safety risk, in which safety risk and/or controls/mitigations:

a. Stay within the Service Unit; the appropriate management official within the Service Unit accepts the safety risk
b. Span Service Units; the appropriate management officials within each affected Service Unit accept the safety risk
c. Go to an LOB outside of the ATO (i.e., to ARP and/or AVS); the appropriate management officials within each affected Service Unit and LOB accept the safety risk

Table 3.8 summarizes risk acceptance requirements.

Table 3.8: Risk Acceptance Summary

Safety Risk and/or Controls:	**High Initial Risk***	**Medium or Low Initial Risk**
	Risk Accepted by:	**Risk Accepted within:**
Stay Within a Service Unit	Service Unit Vice President	Service Unit
Span Service Units	Each Affected Service Unit Vice President	Each Affected Service Unit
Affect LOBs Outside the ATO (e.g., ARP and/or AVS)	Each Affected Service Unit Vice President and Each Associate Administrator	Each Affected Service Unit and LOB

* Note high initial risk must be mitigated to medium or low before acceptance.

Neither Safety Services nor AOV accepts safety risk. Only operational personnel responsible for NAS components can accept risk into the NAS because only they can manage risk by employing controls. However, LOBs outside of the ATO (e.g., ARP and/or AVS) do have a role in accepting safety risk because they are responsible for components of the NAS. Therefore, ATO Vice Presidents, directors, managers, and supervisors work closely with their counterparts in these LOBs to ensure that the appropriate party or parties accept and manage safety risk resulting from NAS changes. It is not possible to implement a change without accepting the risk.

3.15 Tracking Changes

3.15.1 NAS Change Tracking

In addition to the SRMDM and SRMD, each Service Unit must maintain a tracking matrix containing proposed NAS changes within its purview and the related outcome. Table 3.9 provides an example of a form that Service Units can use as a NAS Change Tracking Matrix and the minimum information that is required.

Table 3.9: Example of a NAS Change Tracking Matrix

	Information Regarding the Change					Safety Risk Management Information				
Service Unit	Date Change Proposed	Title of Change	Narrative Description of Change	Accountable Office	Change Approved by	SRMD or SRMDM Developed	Date of SRMD or SRMDM	SRM Point of Contact	SRMD or SRMDM Approved by	Risk Accepted by

3.15.2 NAS Change Tracking Matrix Responsibilities

Safety Services reviews and analyzes the data provided in the NAS Change Tracking Matrix, and when appropriate, provides feedback to the organizations concerning their use of SRM. This analysis assists in identifying the scope of the SRM effort, as well as identifying the resources required to conduct SRM. Safety Services shares the information with AOV; this information helps AOV identify the scope of its oversight effort and provides insight into the processes used by the ATO to improve NAS safety. In addition, each Service Unit is responsible for maintaining its own NAS Change Tracking Matrix and providing monthly updates to Safety Services.

3.15.3 Before Implementing a NAS Change

In addition to SRM, the ATO verifies that a new or modified system (hardware and software) is ready for use in the operational environment for which it is intended. Specifically, the team responsible for the system conducts test and evaluation before implementing a system or a change to the system. It determines the method of verification based on the nature of the change. Through verification, the team shows that the system meets its requirements and performs its intended function(s).

Methods of verification include test, analysis, examination, and demonstration/evaluation. For more information, see the FAA System Engineering Manual and/or the Test and Evaluation Gold Standard on the FAA Intranet.

In addition to verification by the implementing Service Unit, Safety Services' Office of Safety Support and Independent Assessment (SSIA) conducts an independent assessment of operational readiness on designated systems prior to the in-service management phase. For more information on the role of SSIA in SRM, see Sections 4.5.1 - 4.5.2.

3.15.4 SRM Resources

Each Service Unit has a designated Safety Manager who can provide additional guidance regarding the SMS and SRM. In addition, each Service Unit has a Safety Engineer who provides SRM expertise. Both the Safety Manager and Safety Engineer are also available to

provide input to the management official(s) who will accept the risk associated with the change. In addition, if risk is to be accepted outside the Service Unit, the Safety Manager and/or Safety Engineer help facilitate that coordination.

As with any other SMS component or topic in this manual, Safety Services is also available to provide additional guidance and/or information via email at: 9-AWA-ATO-SRM-Safety-Service@faa.gov.

Chapter 4 – Safety Assurance

4.1 Introduction

Safety assurance includes safety reviews, evaluations, audits, and inspections, as well as data tracking and analysis, and investigations. This chapter explains why safety assurance and evaluation are critical to the SMS. It provides a detailed description of assurance programs including the Air Traffic Evaluation and Auditing Program, NASTEP, the IOT&E process, and Safety Services SRM audits—all integral parts of the SMS. This chapter also discusses how the ATO evaluates the SMS and describes safety data tracking and analysis.

4.2 Audits and Evaluations Overview

4.2.1 Audits and Evaluations Defined

Audits and evaluations are scheduled or unscheduled formal reviews, examinations, and verifications of activities, operations, and systems. They are intended to improve the quality of products, processes, or services and provide a means for ensuring compliance with policy and/or contractual requirements. Audits and evaluations also assess the effectiveness of the overall program by identifying areas of positive impact, identifying areas in need of improvement, and verifying the results of those improvements. The scope of audits and evaluations varies with the stage of the program/operation, its maturity, type of safety processes, and level of confidence developed from previous audits. Finally, audits and evaluations contribute to the identification of both positive and negative safety trends, which can lead to the identification and mitigation of hazards.

Audits and evaluations support the essential function of the SMS by ensuring that safety objectives have been met.

4.2.2 Impact on NAS Safety

Audit and evaluation functions proactively look for safety issues and hazards that could lead to incidents and accidents. If ATO employees identify issues or hazards, they resolve/correct them. In some cases, the resolution or corrective action requires a plan to bring it into compliance. In other cases, the resolution or corrective action constitutes a NAS change. An SRM Panel needs to assess such a change using the SRM process, ensuring that it has an acceptable level of risk.

As discussed in Chapter 3, *Safety Risk Management*, there may be instances in which ATO employees discover existing high risk hazards through assurance activities. In those cases, they must follow the process documented in Appendix H, *Documenting Existing Hazards Process*.

4.2.3 Audit and Evaluation Programs

ATO assurance programs evaluate compliance with SMS requirements and FAA and/or ATO orders, standards, policies, and directives. Audit and evaluation programs include, but are not limited to, the following:

a. Air Traffic Evaluation and Auditing Program, run by the Safety Services Safety Assurance Office and outlined in FAA Orders 7010.1S, *Air Traffic Evaluations* and 7210.56, *Air Traffic Quality Assurance*
b. NASTEP, run by the NAS Quality Assurance and Performance Group in Technical Operations Service Management Office and outlined in FAA Orders 6000.15, *General Maintenance Handbook for National Airspace System (NAS) Facilities*; 6040.6, *Airway*

Facilities NAS Technical Evaluation Program; and 6000.30, *National Airspace System Maintenance Policy*

c. Technical Operations Internal Safety Assurance Program (ISA) as outlined in VN Order 1800.1E, *Internal Evaluation Program*
d. Audits of the application of SRM in the Service Units, run by the Safety Services Office of SSIA and outlined in the Safety Risk Management Audit Program Standard Operating Procedure
e. IOT&E and Independent Assessments
f. Service Unit internal audits and evaluations

4.2.4 Audit and Evaluation Methods

A quality evaluation and auditing program involves some basic methods and procedures common to many forms of management reviews. Below are nine common practices used in program evaluation (for safety and/or quality).[13]

a. **Physical Examination (PE)** – This is the activity of gathering physical evidence. It is a substantive test involving the counting, inspecting, gathering, and taking inventory of physical and tangible assets, such as cash, plants, equipment, parameters, etc.
b. **Confirmation** – This is the act of using a written response from a third party to confirm the integrity of a specific item or assertion.
c. **Vouching** – This is the examination of documents that support a recorded transaction, parameter, or amount. Testing starts with the recorded item and moves on to review the supporting documentation.
d. **Tracing** – This technique tracks the source of documents to their accounting records. Tracing is a “through the system” method of accounting transaction flows, “ledgering” accounts, or logging parameters.
e. **Re-performance** – This is an auditing technique of repeating an organizational process or activity with high fidelity and comparing results with previous operational data.
f. **Observation** – This is the process of witnessing physical activities of the organization. It differs from the PE in that the auditor observes the organization performing the organization’s process rather than the auditor performing the examination.
g. **Reconciliation** – This is the process of matching two independent sets of records (independence is an important factor). A derived set of data from the organization does not meet this criterion; only third party or certified independent data meets the criteria. Reconciliation satisfies the test of completeness and existence of evidence.
h. **Inquiry** – This is the technique of asking questions and recording responses.
i. **Inspection** – This is the critical examination of documents (different from vouching or tracing) to determine content and quality of a transaction, such as inspecting leases, contracts, meeting minutes, requirements, organization policy, etc.

ATO employees use auditing techniques to test, validate, and verify processes and metrics obtained and produced by the various entities and organizations in the NAS.

ATO financial or programmatic assessments fall into three categories of audits: financial audits, operational audits, and compliance audits. Each type of audit is described on the following page.

[13] Guy, D. M., Alderman, C. W., and Winters, A. J., *Auditing*, Harcourt Brace Jovanovich Publishers, 1990.

a. **Financial audits** examine accounting and reporting of financial transactions. The purpose of this type of audit is to verify that there are sufficient controls and processes for the acquisition and use of resources.
b. **Operational audits** address the effectiveness and efficiency of the organization. The objective is to determine the organization's ability to achieve its goals, objectives, and mission.
c. **Compliance audits** evaluate or assess conformance to established criteria, process, or work practices. The objective is to determine if employees and processes have followed established policies and procedures.

To ensure quality, ATO organizations currently use both operational and compliance audits and evaluations at the national and operating unit levels. The Office of SSIA primarily uses compliance audits to evaluate the use of and overall effectiveness of the SMS, with a particular focus on SRM. The Safety Services Safety Assurance Office uses both operational and compliance audits to assess established processes, policies, and procedures.

4.2.5 Audit and Evaluation Program Responsibilities

The ATO has internal national assurance programs that evaluate ATC units and equipment. Air Traffic Service Area Directors and Air Traffic Managers (ATMs) are responsible for evaluating their respective facilities annually. The Safety Assurance Office retains oversight of the ATC unit evaluation process, conducts periodic audits of facilities, performs program assessments, and provides assistance to the Service Areas. The NAS Quality Assurance and Performance Group in the Technical Operations Service Management Office runs NASTEP, which is the main component in the overall evaluation and assurance of equipment and maintenance activities; this chapter describes NASTEP starting in Section 4.4.

The Office of SSIA audits the use of the SRM process and its outputs. Safety Services monitors the effectiveness of using safety data to identify and address negative safety trends that impact the provision of ATC and navigation services. Sections 4.6.1-4.6.3 further describe SMS evaluations and audits.

4.3 Air Traffic Evaluations and Auditing Program

4.3.1 ATC Facility Evaluation Program

FAA Orders 7010.1, *Air Traffic Evaluations*, and 7210.56, *Air Traffic Quality Assurance*, describe the current ATC facility evaluation program, which includes evaluations and audits that have compliance and safety perspectives.

4.3.2 Difference Between ATC Facility Audits and Evaluations

Facility personnel conduct evaluations of their facilities each fiscal year, while the Safety Assurance Office (an external party) conducts audits of the facilities according to assigned priorities.

The ATM of a facility conducts an evaluation of his/her facility each fiscal year. He/she may use appropriate means to conduct this evaluation and is not required to complete the evaluation as a single activity. The evaluation team may be composed of any members the ATM deems appropriate and in accordance with all applicable national collective bargaining agreements.

The Safety Assurance Office conducts audits based upon assigned priorities. The office determines priority by soliciting input from the Service Areas and FAA LOBs, as well as by

analyzing objective criteria from sources such as air traffic counts, prior audit and evaluation open items, length of time since last audit, Operational Error/Deviation statistics, other air traffic incidents, etc. The Safety Assurance Office then conducts the audits.

4.3.3 Activities Following an ATC Facility Evaluation or Audit

In accordance with FAA Order 7010.1S, *Air Traffic Control Safety Evaluations and Audits*, the facility submits a Facility Evaluation Report no later than August 1 of each year. It submits this report in the Facility Safety Assessment System (FSAS), Safety Services' national database containing information related to audits and evaluations.

The Facility Evaluation Report includes a list of all items rated "N," "D," or "A," with associated problem statements and mitigation plans. Each ATM and district manager, if applicable, certifies that the report is complete and accurate to the best of his/her knowledge prior to its finalization and input into FSAS.

For audits, the Safety Assurance Office auditor briefs the ATM (or his/her designee) in person or via telephone conference within five calendar days of completing the audit. He/she enters an audit report into FSAS within ten days of audit completion. The audited facility's ATM (or his/her designee) then enters mitigation plans (addressing items rated "N" or "D") in FSAS within 15 calendar days of receipt of the audit report. Any items rated "A" require that the Safety Assurance Office auditor immediately brief the ATM. The ATM then convenes a conference with the appropriate Service Area Quality Assurance Manager and Service Unit Quality Assurance Manager to gain approval for a mitigation plan for that item. The ATM (or his/her designee) then loads it into FSAS.

For both evaluations and audits, the facility submits a status report every 30 days to communicate the status of all items rated less than "M" until the items are raised to the "M" level. The report includes progress on each item including actions, dates, and results.

Upon achievement of the "M" rating for each item, the ATM or his/her designee closes the item in FSAS and obtains concurrence from the Service Area, which he/she then documents in FSAS.

4.3.4 ATC Facility Evaluation and Auditing Program Outcomes

The Service Area and Service Unit personnel who direct work and influence necessary changes identified in the reports review the Facility Evaluation Reports and audit reports created from the evaluations/audits. In addition, the Executive Council reviews synopses of these reports to identify, prioritize, and implement safety enhancing measures. It also tracks this information in FSAS and analyzes it for trends and to target future evaluations, audits, and inspections.

ATO employees can access FSAS via the FAA intranet. To encourage corporate learning, employees can view reports/findings, as well as mitigation plans. For access to FSAS, employees should consult their supervisors.

In addition, the Critical Safety Initiatives (CSI) Group was established within the Safety Assurance Office to develop and communicate initiatives to stakeholders throughout the ATC system. The initiatives are primarily composed of safety awareness products available via the FAA's intranet. They may consist of high fidelity simulations of air traffic scenarios, safety notices, or recommendations to prevent future incidents/accidents and promote a positive safety culture.

4.4 NASTEP

4.4.1 Equipment Evaluation and Auditing Programs

FAA Orders 6000.15, *General Maintenance Handbook for National Airspace System (NAS) Facilities;* 6040.6, *Airway Facilities NAS Technical Evaluation Program;* and 8200.1, *United States Standard Flight Inspection Manual,* describe the equipment evaluation and auditing programs.

NASTEP provides the quality assurance, asset management, and safety decision-making information based on an independent level of review of:

a. How well facilities and services meet their intended objectives
   (1.) Evaluators will check key performance parameters and certification parameters at selected facilities
   (2.) Evaluators will review NAS Performance Analysis (NASPAS) and NAS Performance Index (NASPIX) data
b. How well the maintenance program is executed
   (1.) Evaluators will review facility logs to verify certification and periodic maintenance accomplishment, and documentation of corrective and scheduled maintenance activities
   (2.) Evaluators will review completion of required modifications
   (3.) Evaluators will review facility documentation such as Technical Performance Records (TPR) and required reference data
c. How well customer needs are being met
   (1.) Evaluators will solicit customer feedback through interviews and surveys
   (2.) Evaluators will review the outage coordination process and accuracy
d. Evaluators may also perform reviews of specialist certification records/credentialing. These reviews will be random spot checks of documentation that is geographically convenient to the routine evaluation locations, or conducted as part of a special inspection.

4.5 IOT&E

4.5.1 The Role of IOT&E in SMS

The Safety Services SSIA Office fulfills the agency's commitment to field operationally ready systems by conducting IOT&E prior to the in-service management phase. An IOT&E is a full system-level evaluation conducted in an operational environment to confirm the readiness of a system from an operational and safety perspective before it is incorporated into the NAS. The Vice President of Safety Services directs the commencement of IOT&E following acceptance of an IOT&E Readiness Declaration by the Vice President of the implementing Service Unit. Program Managers from the SSIA Office lead IOT&E Teams, which are staffed by subject matter experts from the organizations that will operate, maintain, or otherwise be operationally affected by the new system or change. These teams assess, document, and brief the operational readiness of designated systems. The teams also verify that the risk ratings of hazards identified in a program's SRMD are accurate, that mitigations are effective, and that no new hazards arise in operational conditions. The teams brief IOT&E assessments to the Vice Presidents of Safety Services, Technical Operations Services, and the implementing Service Unit. They also brief them to the In-Service Decision (ISD) authority in support of ISDs or other acquisition decisions.

4.5.2 IOT&E and SRMDs

The IOT&E Team reviews hazards identified in the SRMD and plans for them in IOT&E as appropriate. Figure 4.1 illustrates the link between the SRMD and the IOT&E process. As a result of the various test activities (as depicted in Figure 4.1), the change proponent should update the SRMD throughout the lifecycle of the system based upon the identification of new safety risks or the effectiveness of the mitigation of existing safety risks.

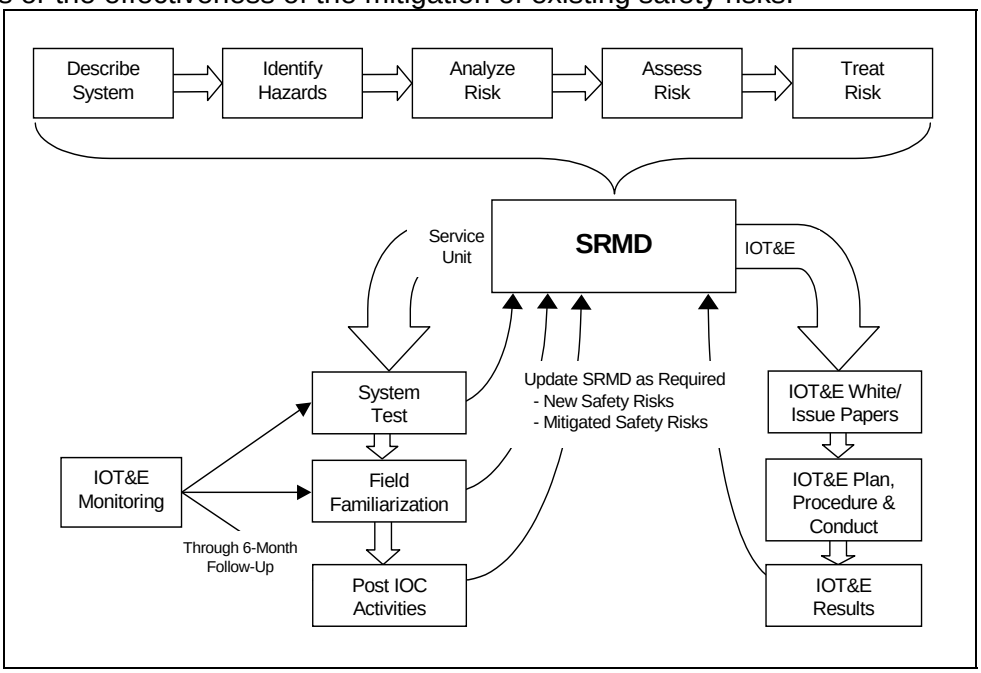


Figure 4.1: SRMD, IOT&E Documentation, and Process Links

4.5.3 SSIA Independent Assessments in SMS

Independent Safety Assessments are a form of SMS evaluations that provide safety data regarding a particular aspect of the NAS. The Vice President of Safety Services or the SMS Director indicates to the Office of SSIA, via a memorandum, which fielded systems, orders, or procedures should undergo Independent Safety Assessments. This selection is based on current safety data, management concerns, or a request from another organization. Independent Safety Assessments are generally operational assessments (facility operations, benefits analyses, operational procedures, order compliance), as opposed to system assessments.

4.6 SMS Evaluations and Audits

4.6.1 Evaluating and Auditing the SMS

In addition to the evaluations, audits, and inspections described already, Safety Services evaluates the overall effectiveness of the SMS. As further described later in this chapter, Safety Services tracks and analyzes safety data for adverse trends and identifies the need for safety enhancing measures. Since the goal of the SMS is to increase the safety of the NAS by meeting or exceeding safety objectives, Safety Services evaluates the SMS on the ATO's ability to manage the safety risks in the NAS and meet these objectives, which are listed in the current FAA strategic plans and the *ATO Business Plan*. As the SMS matures, Safety Services will develop additional metrics to assist in evaluating the effectiveness of the SMS.

Safety Services also audits SMS processes and outcomes. Primarily using compliance audits, Safety Services:

a. Reviews and provides recommendations regarding safety analyses and SRMDs
b. Reviews and provides input on safety risk assessments
c. Reviews and provides input on the results of safety assurance functions within ATO organizations
d. Reviews (and in some cases, develops) safety data analysis reports
e. Analyzes safety data and advises ATO and FAA management on safety-related issues

As discussed in Chapter 3, *Safety Risk Management*, the ATO uses a web-based hazard tracking system to track all hazards. The information is maintained throughout the lifecycle of a system or change and updated until the level of risk is mitigated to low. Hazard tracking, in part, includes documenting safety requirements, providing the status of requirements validation and verification, verifying implementation, and updating the current and predicted residual risk levels before acceptance. The monitoring plan included in the SRMD establishes cycles in which existing and implemented mitigations are assessed for effectiveness.

Through safety assurance efforts, Safety Services oversees the ATO audit processes, which evaluate the implementation and effectiveness of risk mitigations. There are times when audits identify mitigations to be ineffective in reducing the risk to an acceptable level. When this occurs, the change proponent and/or SRM Panel must reapply the SRM principles by identifying potential (new or unmitigated) hazards, assessing the associated risk of the hazards, developing mitigation strategies for treating the risk, and documenting their analysis within an amendment to the SRMD. Hazards are tracked and mitigations monitored throughout the lifecycle of the system or change or until the level of risk is mitigated to low.

4.6.2 Evaluating SRM Usage

Safety Services primarily uses audits to evaluate the use of SRM. The auditors review the resultant documentation of NAS changes. These include, but are not limited to:

a. NAS change tracking information
b. Hazard tracking system
c. SRMDs and SRMDMs

Each program or organization that is deemed to be SRM-compliant is a potential candidate for audit by the Safety Services SSIA Office. In this context, SRM-compliant means that the program or organization has received the appropriate training and support necessary to reasonably be expected to meet the SRM requirements of the SMS. The SSIA Office, in conjunction with the appropriate Service Unit Safety Manager, makes this determination.

4.6.3 SRM Audit Process

SRM audits are conducted to determine if the Service Units are implementing and integrating SRM into existing processes, procedures, and NAS changes, as required by ATO Order JO1000.37, *Air Traffic Organization Safety Management System,* and stated in the guidance provided in the SMS Manual, the SRMGSA, and other associated orders and SMS Implementation Plans. SRM audits are also conducted to determine how well the elements of SMS (i.e., safety policy, SRM, safety assurance, and safety promotion) are implemented within the ATO.

The SRM Audit Program Manager designates an ISO 9001 Lead Auditor for each audit. The team lead works with the SRM Audit Program Manager to identify the other members of the SRM audit team. The audit team reviews documentation and compares that documentation to requirements (criteria) identified for the audit. The audit team creates questionnaires for on-site interviews tailored to the audit subject. If necessary, all audit team members conduct interviews.

Upon selection of the audit subject, the Service Unit is notified of the upcoming audit. The audit team conducts an introductory telephone conference to introduce the audit team and to request the management or program goals for the audit. During the telephone conference, the audit team lead establishes the audit schedule with the Service Unit management Point of Contact (POC). The schedule includes the entrance briefing, the interview schedule, daily briefings with the POC, and the exit briefing.

Once on-site, the audit team lead conducts the entrance briefing to introduce the audit team members and review the audit process. The management POC introduces the appropriate audit participants and states the goals for the audit.

The audit team conducts on-site interviews, by telephone if necessary, and documents audit findings. Each day, the audit team lead presents the audit findings to the POC.

Audit findings are identified as Non-Conforming Findings (NCFs), Opportunities For Improvement (OFIs), or Positive Observations (POSs). NCFs are specific instances in which the application of SRM (or lack of application) clearly does not meet requirements. OFIs are instances in which it cannot be determined whether the requirements have been met. The opportunity exists for the organization audited to improve on processes or procedures currently in place to meet the requirements. POSs are best practices or activities that reflect proactive SRM integration. Findings are documented and shared with management.

The audit team lead conducts the exit briefing with the appropriate Service Unit Safety Manager and/or designee, the lead of the program or organization being audited, the management POC, and anyone else deemed appropriate. The team lead presents the audit findings at the exit briefing. Should NCFs be identified, the audited organization is responsible for completing a Corrective Action Plan (CAP).

The CAP includes the items that did not meet the safety requirements, the actions needed to meet the requirements, and timelines for conducting the corrective action. A CAP must be submitted between 30 and 60 days after the final audit report, depending on the severity and/or complexity involved in responding to and/or correcting the NCF. For example, a CAP for a Configuration Management change to a document would be required in 30 days. If the SRM Audit report found no items requiring corrective action, no CAP is necessary.

Safety Services provides a printed and an electronic copy of the SRM audit report to the Director of the Service Unit audited within 30 business days of the exit briefing. The Service Unit Director signs the report within 10 days of receiving the finalized document.

4.7 Safety Data Tracking and Analysis

4.7.1 Safety Data Tracking and Analysis Introduction

This section discusses the importance of safety data, the types of safety data, and how personnel collect and report it. It describes the processes for reporting safety incidents and

accidents and the relationship between incident investigations and SRM. It also details existing safety data reporting documents and processes.

4.7.2 Purpose of Safety Data Collection and Evaluation

A critical component of the SMS is tracking and analyzing safety data to enhance the ATO's awareness of potentially hazardous situations. The SMS and Safety Services assist with the collection and analysis of agency-wide safety data and support the sharing of the data to continually improve the safety of the NAS.

The safety data are used to:

a. Identify risks and verify the effectiveness of implemented controls
b. Identify areas in which safety could be improved
c. Contribute to accident and incident prevention
d. Assess the effectiveness of training

4.7.3 Safety Services' Role in Safety Data Collection and Evaluation

Safety Services leverages safety data available through various sources within and outside the FAA. Safety Services analyzes safety data to identify adverse trends and identify indicators of potential safety issues. Over time, these data will help identify early indicators that point to potential problems in the system. Safety Services uses safety data to assess the effectiveness of the SMS by tracking safety metrics to produce reports on NAS safety.

4.7.4 Existing Safety Data Collection and Reporting Processes

Currently, the FAA collects and reports safety data from a wide range of sources in the NAS. Table 4.1 (in Section 4.7.12 of this chapter), lists many of the existing FAA and/or ATO orders, processes, and databases related to safety data collection and reporting.

FAA Order 7210.56, *Air Traffic Quality Assurance,* provides specific direction regarding the recording, reporting, and investigation of air traffic incidents.

FAA Order 6040.15, *National Airspace Performance Reporting System,* and FAA Order 6000.30, *National Airspace System Maintenance Policy,* cover reporting on serviceability of ATO facilities and systems, such as failures and degradations of communications, surveillance, and other systems and equipment that impact safety. Maintenance guidelines, directives, checklists, configuration management, and NASTEP contribute to the periodic review and maintenance of equipment and procedures.

The *Safety Recommendation Reporting System* provides FAA Aviation Safety Inspectors a method to develop and submit safety recommendations directly to the Office of Accident Investigation (FAA Order 8020.16, *Air Traffic Organization Aircraft Accident and Incident Notification, Investigation, and Reporting*).

Several non-punitive, voluntary reporting programs, such as the Aviation Safety Action Program (ASAP), the National Aeronautics and Space Administration's (NASA's) Aviation Safety Reporting System (ASRS), the FAA's Aviation Safety Reporting Program (ASRP), and Near Midair Collision System (NMACS) allow pilots and/or air traffic controllers to report an incident or event. Often, if the pilot reports an event within 24 hours, he/she is protected against further actions. The programs are designed to foster better reporting and higher quality data.

The FAA also has mechanisms for employees to report issues, including the Unsatisfactory Condition Report (UCR) program, the Aviation Safety Hotline, and the Administrator's Hotline (both hotlines can be reached by calling 1-800-255-1111). To find out more about these programs, refer to Section 4.7.10 in this chapter.

4.7.5 Safety Incident and Accident Reporting Process

Within three hours of an incident, facilities report it to the Safety Services Safety Assurance Office using a *Preliminary Operational Error/Deviation Investigation Report*. Within one hour of receiving the report, the event is scored according to its severity, based on vertical and horizontal separation and whether or not it was a controlled or uncontrolled incident. The scores range from A to C. Facility employees finalize the preliminary report and the preliminary severity rating into a *Final Operational Error/Deviation Report* within 45 days. Additionally, the National Operations Control Center (NOCC) and TechNet are potential sources of supporting data for use during evaluation of OEs.

For surface incidents, facilities forward the data to the Safety Services Office of Runway Safety and the Office of Operational Services. Authorities score the event based on the collision risk of the incident. Similar to airborne events, authorities apply a score of A to D, produce a report, and make that report available within one week of the event.

Each day, the *Administrator's Daily Alert Bulletin* summarizes incident reports. The briefings report, track, and analyze trends, which are reported to FAA and ATO leadership.

If personnel identify a pilot deviation, they inform the Flight Standards District Office (FSDO), which investigates the event to determine what further action is needed.

Figure 4.2 depicts the incident reporting process.

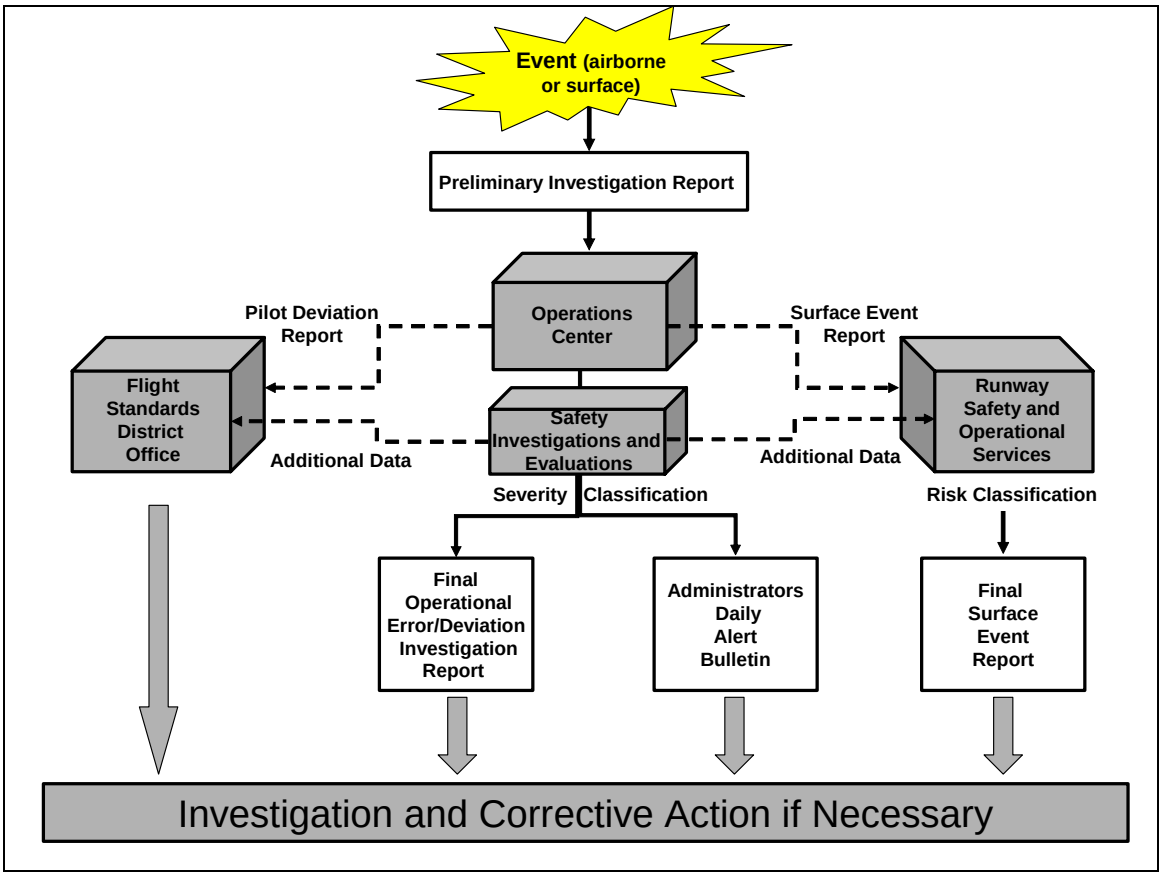


Figure 4.2: Incident Reporting

4.7.6 How Incident Reporting Enhances Safety

The reporting of events leads to investigations. ATO employees conducting the investigation reconstruct and analyze the event. During reconstruction, they identify contributors to the event and characterize them as either direct or indirect. They also identify factors that may have lessened the impact of the occurrence. They analyze all of these factors for severity and often relate them to the SRM process. Then, they use this information as input to develop recommended mitigation strategies and safety-enhancing measures to preclude similar events in the future.

Safety professionals implement corrective action to enhance safety at all levels, from national to local, and they continuously track data to identify improvement or degradation trends.

Safety professionals review data and analyze trends, which may lead to:

a. Airspace and airport improvements
b. Additional Communications, Navigation or Surveillance (CNS) systems, and/or automation systems
c. Additional staffing
d. Other safety-enhancing changes

4.7.7 Incident Investigation Related to Hazard Analysis and SRM

Experience has shown that for every catastrophic accident there are many precursor incidents or minor accidents. For each incident, there are numerous precursor hazards. There are

organizations that have mature processes to investigate accidents (e.g., NTSB, FAA Office of Accident Investigation (AAI)) and conduct analyses that proactively look for potential hazards. However, accident prevention programs focus on the collection, analysis, and investigation of incident data.

Incident investigation is valuable because of two critical characteristics:

a. It reflects real-world occurrences that can be analyzed to prevent or eliminate future occurrences
b. If data are immediately and adequately collected, the information about the incident is intact and not destroyed

The SMS requires the collection and analysis of incident data to determine if hazards exist. It also requires that the risk of those hazards be managed with the intent of preventing future accidents. The key is developing the capability to sort and analyze the vast array of data and transform it into useful information that permits the identification and mitigation of hazards.

4.7.8 Reported Safety Data About Serviceability of Equipment, Systems, and Facilities

Outage reports, significant event reports, and general maintenance logs capture the majority of daily system performance metrics (including incident reporting). ATO employees make additional reports in the form of NOTAMs and accident reporting. Additionally, they collect data via a formal hotline and through the UCR program (described in Section 4.7.10 of this chapter). They consolidate outage and incident data into a daily report developed for the Office of the Administrator.

4.7.9 How Serviceability Reporting Enhances Safety

Equipment installed in the NAS used for aircraft separation has established performance metrics necessary for system safety. The monitoring of overall trends and performance levels is accomplished systematically and documented via its certification. FAA Order 6000.30, *National Airspace System Maintenance Policy*, states, “Certification is a quality control method used to ensure NAS systems and services are performing as expected” (paragraph 11d).

The NASTEP and UCR programs require written documentation and management involvement in the review, mitigation, and analysis of trends. Through NASTEP, personnel conduct periodic independent technical reviews of services provided by system, sub-system, and equipment. These reviews also address how well the services match customer needs.

4.7.10 Data That Should Be Reported

The processes listed above describe reporting of specific types of safety data. However, over and above the reporting of this data, it is important that each employee reports any occurrence or situation that he/she thinks is, or could become, a hazard within the NAS. The ATO safety culture depends upon this voluntary reporting.

The FAA has formal mechanisms for employees to report issues, including the UCR program, the Aviation Safety Hotline, and the Administrator’s Hotline.

The UCR program (FAA Order 1800.6, *Unsatisfactory Condition Report*) is a direct means of advising management of an existing unsatisfactory condition. The UCR process has a defined feedback loop that requires the responsible organization to complete the review cycle and

respond within 30 calendar days to the submitter. The UCR cannot be closed until the condition described in the report is resolved nor can it be closed based on planned actions.

The Aviation Safety Hotline (1-800-255-1111) is for reporting possible violations of Title 14 of the Code of Federal Regulations (14 CFR) or other aviation safety issues, such as improper record keeping, non-adherence to procedures, and unsafe aviation practices. The Hotline is described in FAA Order 8000.73, *Aviation Safety Hotline*. If a caller requests confidentiality, caller identity or information in the report concerning an individual is protected from release under the Privacy Act. If the caller requests feedback and has provided his/her name and address, he/she receives a written response after the issue is closed. Similar to the UCR process, issues are closed within 30 days of the report.

The Administrator's Hotline operates in the same fashion as the Aviation Safety Hotline. It can also be reached at 1-800-255-1111. After dialing the hotline number, a menu directs callers in the appropriate direction. The main operational difference between the two hotlines is that issues reported to the Administrator's Hotline are closed within 14 days of the report.

4.7.11 Where to Report Safety Concerns

As part of the ATO safety culture, ATO staff should report safety concerns to their supervisors. In such cases, supervisors require employees to document as much information as possible about the concern. If an existing FAA and/or ATO order covers the type of safety issue being reported, personnel follow the procedures outlined in that order.

If none of the orders or programs apply to a particular safety concern, employees should report the issue to their immediate supervisor. If the supervisor deems it necessary, he/she reports the issue to Safety Services for analysis. The supervisor reporting the concern receives feedback on the outcome of the analysis.

4.7.12 Safety Data Locations

FAA employees populate several aviation safety databases (see Table 4.1) with information regarding NAS safety events and serviceability. The following paragraphs describe several of the databases.

The National Airspace Incident Monitoring System (NAIMS) database houses collected and categorized safety events. The Safety Assurance Office maintains a database that provides severity classifications for airborne Operational Errors. The Office of Runway Safety and the Office of Operational Services categorize surface events that include surface Operational Errors, Operational Deviations, and pilot, vehicle, and pedestrian deviations. AAI investigates and tracks aircraft accidents and publishes monthly reports.

Air traffic facilities report pilot deviations; the Safety Assurance Office reviews them for air traffic involvement; and AFS investigates and tracks them.

Flight crews report Near Midair Collisions (NMACs) to air traffic facilities; the Safety Assurance Office reviews them for air traffic involvement; and AFS investigates and tracks them. This information is stored in the NMACS database.

The Aviation Safety Information Analysis and Sharing System (ASIAS) enables integrated queries across multiple databases, allowing users to search the warehoused safety data and display queries in useable formats.

Many professionals utilize the aviation safety data to develop safety enhancements to the NAS. Other methods for gathering safety data to identify potential safety enhancements include:

a. NTSB recommendations
b. Requirements for new CNS and/or automation services to enhance or expand airspace management
c. UCRs (as discussed earlier)
d. Employee suggestions
e. Applications for procedural changes
f. Research and development
g. Acquisition of new systems (hardware and software) and equipment
h. Industry advocacy
i. Participation in international forums
j. SRM process documented in this manual

Table 4.1: Safety Data Reporting Documents and Processes

FAA Orders and Processes Related to Safety Data Reporting		
Type of Data/System Name	**Overview**	**References**
Mandatory Reporting Data		
Air traffic incidents	This order mandates that personnel collect and analyze data concerning air traffic incidents.	FAA Order 7210.56, *Air Traffic Quality Assurance*
Aircraft accident/incident	This order contains reporting requirements regarding safety issues, concerns, incidents, and accidents.	FAA Order 8020.16, *Air Traffic Organization Aircraft Accident and Incident Notification, Investigation, and Reporting*
System outages	This order mandates outage reports and contributes to the daily system performance and incident reporting.	FAA Order 6040.15, *National Airspace Performance Reporting System*
Significant system events	This order mandates the reporting of significant events and contributes to the daily system performance and incident reporting.	FAA Order 6030.41, *Notification Plan for Unscheduled Facility and Service Interruptions and Other Significant Events*
Unsatisfactory condition	This order provides Agency employees a means of advising management of unsatisfactory conditions.	FAA Order 1800.6, *Unsatisfactory Condition Report RIS*
Oceanic Altitude/Navigation Errors	This order establishes procedures for processing reports and for collecting system data for analysis.	FAA Order 7110.82, *Monitoring of Navigation, Longitudinal Separation and Altitude Keeping Performance in Oceanic Airspace*
Safety recommendations	This order establishes procedures for Aviation Safety Inspectors to report safety recommendations directly to AAI.	FAA Order 8020.16, *Air Traffic Organization Aircraft Accident and Incident Notification, Investigation, and Reporting*

FAA Orders and Processes Related to Safety Data Reporting		
Type of Data/System Name	**Overview**	**References**
Aviation Safety Information Analysis and Sharing System (ASIAS)	ASIAS is a data warehouse and integrated database system. It enables users to perform queries across multiple databases and display queries in useful formats.	http://www.asias.faa.gov
National Airspace Incident Monitoring System (NAIMS)	This database is in which safety events are collected and categorized.	
Safety Services Office of Runway Safety and Office of Operational Services	The Office of Runway Safety and the Office of Operational Services categorize surface events that include surface Operational Errors/Deviations, and pilot, vehicle, and pedestrian deviations.	
Accident/Incident Data System (AIDS)	The FAA AIDS database contains accident and incident data records for all categories of civil aviation.	AVS is the custodian of the AIDS database.
NTSB Accident/Incident Database	The NTSB accident/incident database is the official repository of aviation accident data and causal factors. In this database, personnel categorize events as accidents or incidents.	
Operational Error and Deviation System (OEDS)	ATO employees use this system to determine if actions of a controller resulted in a loss of separation or an aircraft landing or departing on a closed runway.	
Pilot Deviation System (PDS)	The FAA uses this system to determine if actions of a pilot violated regulations.	
Facility Safety Assessment System (FSAS)	This national database contains reports/findings and mitigation plans from the Air Traffic Evaluation and Auditing Program.	Maintained by Safety Services
Integrated NASTEP Application (INA)	This national database contains reports/findings and mitigation plans from NASTEP audits and evaluations.	Maintained by the NAS Quality Assurance and Performance Group in Technical Operations Services Management Office
Hazards related to the acquisition and implementation of new systems; HTS, FAST and the AMS	These systems are designed to identify, eliminate, or resolve determined or assigned risk, estimate a likelihood of occurrence, and track hazards throughout the lifecycle of a program.	HTS, FAST, and the AMS

FAA Orders and Processes Related to Safety Data Reporting		
Type of Data/System Name	**Overview**	**References**
Voluntary Reporting Data		
Aviation Safety Reporting System (ASRS) and Aviation Safety Reporting Program (ASRP)	ASRS and ASRP are voluntary programs designed to encourage the identification and reporting of deficiencies and discrepancies in the airspace system. NASA receives, processes, and analyzes raw data, which ensures the anonymity of the reporter and of all parties involved in a reported occurrence or incident. Consequently, this increases the flow of information necessary for the effective evaluation of the safety and efficiency of the system.	Advisory Circular 00-46, *Aviation Safety Reporting Program*
Aviation Safety Action Program (ASAP)	This program is a voluntary reporting of safety issues and events that come to the attention of employees of certain certificate holders. To encourage employees to voluntarily report safety issues even though it may involve an alleged violation of 14 CFR, the program includes enforcement-related incentives.	Advisory Circular 120-66, *Aviation Safety Action Program (ASAP)*
Near Midair Collision System (NMACS)	It is the responsibility of pilots and/or flight crew members to determine whether a NMAC actually occurred and if so, initiate a NMAC report. There is, however, no regulatory or legal requirement that a pilot and/or flight crew report a NMAC event, although they are encouraged to do so.	This program is administrated by AVS.
Global Aviation Information Network (GAIN)	The GAIN, an industry-led international coalition of airlines, manufacturers, employee groups, governments, and other aviation organizations, was formed to promote and facilitate the voluntary collection and sharing of safety information.	This program is administrated by AVS.
Automatic Reporting Data		
Incident and maintenance reporting in Maintenance Management System (MMS)	The MMS contains general maintenance logging, which contributes to the daily system performance and incident reporting.	FAA Order 6000.48, *General Maintenance Logging Handbook*

4.7.13 Impact of Safety Data Tracking and Analysis on NAS Safety

ATO employees use safety data tracking and analysis to proactively look for negative trends or safety issues and hazards that could lead to incidents and accidents. If they identify issues or hazards, they resolve/correct them. In most cases, the resolution or corrective action would constitute a NAS change, which would require the use of the SRM process to meet an acceptable level of risk. This is an example of creating a closed-loop process for managing safety.

Chapter 5 – Safety Promotion

5.1 Introduction

This chapter provides detail on a critical aspect of the SMS—safety promotion. Safety promotion is about communicating and disseminating safety information to strengthen the safety culture and support integrating the SMS into all elements of the ATO. Safety promotion includes safety culture, safety lessons learned, reporting systems, recommendations based on safety metrics, and safety training. The general intent of safety promotion is to foster a positive, safety culture in which ATO employees receive ongoing training and updates of safety progress; feel comfortable and compelled to report safety issues or concerns; and understand both why safety is important and how they impact it. Through safety promotion, senior managers broadcast their commitment to safety and the SMS. With this demonstrated commitment, employees recognize the importance of safety. Through additional safety promotion activities, employees understand their role in safety and its impact on the NAS.

This chapter discusses what a safety culture is, its importance, and individual responsibilities, values, and behaviors. It also describes SMS training, including available courses, topics addressed, intended audiences, and delivery methods.

5.2 Safety Culture

5.2.1 Safety Culture Definition and Importance

The ATO and AOV define **safety culture** as the product of individual and group values, attitudes, competencies, and patterns of behavior that determine commitment to, and the style and proficiency of, an organization's health and safety management. In addition, the four key components of a positive safety culture are *reporting* (encourage employees to divulge information about all hazards that they encounter), *just* (employees are encouraged and rewarded for providing essential safety-related information but are held accountable for deliberate violations of the rules), *flexible* (to adapt effectively to changing demands and allow quicker, smoother reactions to off-nominal events), and *learning* (willing to change based on safety indicators and hazards uncovered through assessments, data, and incidents).

Individual efforts alone do not necessarily result in the desired outcome. An organization will realize a positive safety culture only when it develops an aggregate attitude that is manifested by a pervasive type of safety thinking. This type of organizational thinking will permit the individual to have an inherently questioning attitude, a resistance to complacency, a commitment to excellence, and a sense of personal accountability. The cumulative effect of these organizational and individual attitudes develops a corporate attitude of self-regulation in safety matters. This transformation will occur only when leadership provides a vibrant, encouraging atmosphere in which it fosters individual growth and recognizes and rewards the right behavior.

Thus, safety culture is both attitudinal as well as structural in nature, relating to both individuals and organizations. It is about not only identifying safety issues, but also matching them with appropriate actions.

A positive safety culture is focused on finding and correcting systemic issues rather than finding someone or something to blame. A positive safety culture flourishes in an environment of trust, encouraging error-reporting and discouraging covering up mistakes. The need to address behavior that is malicious or recklessly negligent must be balanced with the need for a just culture that is not excessively punitive. A positive safety culture goes beyond simply adhering to

procedures. It is demonstrated when employees carry out their duties correctly, with alertness, due thought and full knowledge, sound judgment, and a proper sense of accountability.

A safety culture supports the tenets of the SMS since all employees understand their unique significance in the safety of the NAS. All employees give safety the highest priority in every decision that they make, and each employee understands the safety consequences of his/her actions.

5.2.2 Positive Safety Culture Values

What the people in an organization do defines its culture. Organizational values can be judged by decision-makers' actions. For instance, the extent to which managers and employees act on commitments to safety demonstrates the values that motivate their actions. To foster a positive safety culture, management sets the standards by allocating adequate resources, providing unambiguous policy direction, and promoting open communication. Safety training (discussed later in this chapter) is an especially important activity for strengthening the organizational safety culture. The following values are inherent in a positive safety culture:

a. Employees at all levels understand the hazards and risk inherent in their operations and those with whom they interface.
b. Employees continuously work to identify and control/manage hazards or potential hazards.
c. Employees understand errors, make efforts to eliminate potential errors from the system, and do not tolerate willful violations.
d. Employees and management understand and agree on what is acceptable and unacceptable.
e. Management encourages employees to report safety hazards.
f. When employees report hazards, others can analyze them using a hazard-based methodology and take appropriate action.
g. Employees track hazards and actions to control them and report them at all levels of the organization.
h. Management encourages employees to develop and apply their own skills and knowledge to enhance organizational safety.
i. Staff and management communicate openly and frequently concerning safety hazards.
j. Employees widely distribute/make available safety reports so that everyone learns the lessons.

5.2.3 Positive Reporting Culture

A positive reporting culture reinforces a safety culture. An organization with a positive reporting culture is one in which:

a. The reporting system is simple and user-friendly.
b. Management encourages the reporting of safety occurrences.
c. Employees see the treatment of staff who submit safety reports as just.
d. Managers/evaluators investigate each occurrence report received.
e. Report recipients provide feedback to the originator of the report.
f. Management ensures that the submission of reports results in corrective action to prevent recurrence.
g. Managers maintain confidentiality, insofar as possible, in relation to disclosure of information concerning individuals.
h. Management disseminates lessons learned to all staff.

Effective communication of the risk is critical and a key component of the safety culture. When reporting on the risk, the communication should:

a. Raise the level of understanding of relevant issues
b. Stick to the facts
c. Focus on what the audience knows
d. Be tailored to audience needs
e. Place the risk in the appropriate context
f. Present the risk in order of concern
g. Be respectful in tone
h. Be forthright about any limitations
i. Deal with trust and reliability
j. Be focused on specific issues

A positive safety culture depends on voluntary reporting. Management is essential in supporting and encouraging reporting behavior to be effective. Within a positive safety culture, effective leaders:

a. Allocate resources to safety management
b. Encourage a questioning attitude regarding safety
c. Recognize to err is human
d. Do not tolerate willful violations of safety policies/rules
e. Foster open communication regarding potential safety hazards
f. Encourage employees to develop and apply their own skills and knowledge to enhance organizational safety
g. Recognize individual and organizational safety accomplishments
h. Present safety lessons learned to all employees

Within a positive safety culture, employees:

a. Look for potential safety hazards
b. Report potential safety hazards
c. Openly discuss safety hazards and seek support to mitigate them
d. Work to reduce safety hazards within their purview

5.2.4 Agency-wide Safety Data Sharing

Single events rarely cause accidents and incidents; rather, accidents and incidents are a function of multiple events. In a system as large and diverse as the NAS, the numerous organizations responsible for its components each have a different perspective. Events often fall in the purview of multiple organizations. Sharing safety data and analyses assists the ATO in identifying issues that are the result of events on which only one organization within the ATO would normally focus. ATO organizations can also benefit by sharing safety data with and from international Air Traffic Service (ATS) providers.

Some of the databases (e.g., ASIAS and NAIMS) described in Chapter 4, *Safety Assurance*, consolidate data from multiple sources and provide an Agency-wide perspective.

5.2.5 Dissemination of Lessons Learned

The SMS is an evolutionary and constantly maturing system. As it matures, safety processes will become more refined and more ingrained into existing ATO processes and procedures. Dissemination of lessons learned will expedite its maturation by identifying and resolving problems and issues rather than allowing them to be repeated. Sharing lessons learned also fosters an ATO-wide perspective on decision-making and improves the efficiency of the SMS and the NAS.

An important function of Safety Services is to facilitate the documentation, collection, and distribution of lessons learned. Appendix C, *ATO Safety Guidance Process*, contains information related to the safety guidance process, which is a mechanism for disseminating lessons learned and other SMS guidance material to the ATO.

5.2.6 Impact of Organizational Factors on Safety

Organizational factors, such as training, documentation, and working environment impact safety. Employees must be adequately trained, documentation must be complete and up-to-date, and the working environment must be conducive to the work being performed. However, some less obvious organizational factors, like structure or attitude, also affect safety. For instance, open communication is conducive to safety. If an organization is too complex or the attitude is such that information is not shared readily or willingly, safety could suffer.

5.2.7 Measuring or Assessing a Safety Culture

The culture of an organization or facility is a complex entity, but it is possible to measure the safety climate by asking employees how comfortable they are in reporting errors and how much management encourages adherence to procedures. Organizations outside the FAA have used standardized surveys with five-point scales to score and characterize the safety climate of organizational units, allowing comparison of a facility against national norms or against like organizational units. Relatively low scores have been correlated with higher error rates; the questions in the survey have helped pinpoint underlying causes of error rates. The importance of measuring and tracking ATO safety culture improvements is articulated in ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*. The ATO conducts a Safety Culture Survey each year; based on the survey results, the ATO will develop Safety Climate Assessment Action Plans to drive meaningful improvements in safety culture across the organization.

5.2.8 Safety Services' Role in Promoting Safety Culture

All Service Units have a role in promoting safety culture in the ATO. Safety Services takes the lead role in coordinating promotion efforts. It documents the current safety culture and facilitates cross-organizational communication and coordination, safety data sharing, and dissemination of lessons learned. Safety Services also provides input from a safety perspective to decision-makers.

5.3 SMS Training

5.3.1 Training Overview

Training is another important component of safety promotion. It is a means for sharing information about the SMS and providing the skills and knowledge needed to carry out SMS responsibilities. Employees receive information and training on SMS concepts, processes, and guidance at a level that commensurate with their job functions as they relate to the SMS. Safety

Services and the other Service Units have designed, developed, and delivered several training courses aimed at various audiences including:

a. Introduction to the SMS
b. Manager's Role in SRM
c. SRM Training
d. SMS/SRM Terminal Operations Implementation Workshop (Item Number FAA67000001)
e. SMS Briefing for Terminal Managers (Item Number FAA67000002)
f. En Route and Oceanic Services SRM Panel Facilitation

Each course is described below.

5.3.2 Introduction to the SMS

Introduction to the SMS (Item Number FAA10603) is a one-hour web-based course available through the Department of Transportation (DOT) eLearning Management System (eLMS). It provides an overview of the ATO SMS, including information on SMS components and concepts, as well as roles and responsibilities. The course applies to all ATO employees and support contractors who are involved with the provision of ATC and navigation services. Course topics include:

a. SMS overview
b. AOV
c. Safety policy
d. SRM
e. Safety assurance
f. Safety promotion
g. SMS implementation
h. Employee roles and responsibilities

5.3.3 Manager's Role in SRM

The Manager's Role in SRM (Item Number FAA66000001) is a one-hour web-based course available through eLMS. The Introduction to the SMS course is a prerequisite for this course. The Manager's Role in SRM provides a better understanding of the managers' roles and responsibilities related to the SRM process. The intended audience includes all ATO executives, managers, and supervisors who approve changes to the NAS and are in positions to accept the risk of those changes and/or approve SRMDs and SRMDMs. Course topics include:

a. SRM process
b. Managerial roles and responsibilities with respect to SRM and NAS changes
c. Differences between an SRMD and SRMDM
d. Differences between approving an SRMD and accepting the risk of the NAS change
e. NAS change approval levels and risk acceptance levels associated with SRM
f. Compliance process

5.3.4 SRM Training

SRM Training (Item Number FAA66000004) is a two-day classroom course that provides detailed information on SRM and its uses, tools/techniques primarily used in SRM, and documentation requirements. This training is required for employees who make changes to the

NAS that could reasonably impact NAS safety, including those who conduct safety analyses and/or are responsible for any component of SRM when making changes to the NAS. The Introduction to the SMS course is a prerequisite for this course. Course topics include:

a. SMS overview and its importance
b. Characteristics of a safety culture
c. Roles and responsibilities within the SMS
d. SRM concepts and terms
e. SRM process
f. Tools/techniques primarily used in SRM
g. Identification of what level of safety analysis is required under SRM
h. Documentation requirements for changes
i. Development of controls and safety risk mitigation strategies
j. Development of monitoring mechanisms for controls and safety risk mitigation strategies
k. Development of SRMDs
l. Risk acceptance and SRMD approval processes

5.3.5 Additional Information on SMS Training

Service Unit Safety Managers and Safety Engineers are the first points of contact for additional information on the SMS, including training. Safety Services can also provide more information about SMS training and can be contacted at 9-AWA-ATO-SRM-Safety-Service@faa.gov.

Appendix A – Glossary of Terms

(These definitions are consistent with those included in AOV SOC 08-06, ATO Safety Management System (SMS) Definitions; Safety Risk Management Guidance for Systems Acquisitions; FAA Advisory Circular AC25.1309; System Design Analysis; and other FAA documents.)

Accident. An unplanned event that results in a harmful outcome; e.g., death, injury, occupational illness, or major damage to or loss of property.

AOV Acceptance. The process whereby the regulating organization has delegated the authority to the service provider to make changes within the confines of approved standards and only requires the service provider to notify the regulator of those changes within 30 days. Changes made by the service provider in accordance with their delegated authority can be made without prior approval by the regulator.

AOV Approval. The formal act of responding favorably to a change submitted by a requesting organization. This action is required prior to the proposed change being implemented.

Assessment. An estimation of the size/scope of risk or quality of system or procedure.

Assumptions. Characteristics or requirements of a system or system state that are neither validated nor verified.

ATC Zero. A total loss of ATC capability and the complete loss of control services.

Bounding. A process of limiting the analysis of the proposed change or system to the elements that affect or interact with each other to accomplish the central mission or function of that change or system.

Cause. Events that, result in a hazard or failure. Causes can occur by themselves or in combinations.

Change. To modify, alter, or make different.

Common Cause Failure. A failure that occurs when a single fault results in the corresponding failure of multiple system components or functions.

Concurrence. An agreement with results or conclusions expressed in a change justification SRMDM, SRMD, or other documentation. Note: Due to the nature of how Air Traffic Control procedures are employed and evaluated the verification process is confirmed after implementation of the procedure.

Configuration Management. A management process for establishing and maintaining consistency of a product's performance, functional and physical attributes with its requirements, design, and operational information throughout its life.

Control. Anything that mitigates the risk of a hazard's effects. A control is the same as a safety requirement. All controls are written in requirement language. There are three types of controls:

(1) **Validated.** Those controls and requirements that are unambiguous, correct, complete, and verifiable.

(2) **Verified.** Those controls and requirements that are objectively determined to have been met by the design solution.

(3) **Recommended.** Those controls that have the potential to mitigate a hazard or risk, but have not yet been validated as part of the system or its requirements.

Critical NAS System. A system that provides functions or services that if lost would prevent users of the NAS from exercising safe separation and control over aircraft.

Effect. The effect is a description of the potential outcome or harm of the hazard if it occurs in the defined system state.

Equipment. A complete assembly, operating either independently or within a sub-system or system, that performs a specific function.

Error Tolerant System. A system designed and implemented in such a way that, to the maximum extent possible, errors and equipment failures do not result in an incident or accident.

Facility. Generally, any installation of equipment designated to aid in the navigation, communication, or control of air traffic. Specifically, the term denotes the total electronic equipment, power generation, or distribution systems and any structure used to house, support, and/or protect these equipment and systems. A facility may include a number of systems, sub-systems, and equipment.

Hazard. Any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. A hazard is a condition that is a prerequisite to an accident or incident.

Hazard Tracking. A closed-loop means of ensuring that the requirements and mitigations associated with each hazard that has associated medium or high risk are implemented. Hazard tracking is the process of defining safety requirements, verifying implementation, and re-assessing the risk to make sure the hazard meets its risk level requirement before being accepted.

Human-Centered. The structured process during concept and requirements definition, design, development, and implementation that identifies the user as the focal point of the effort for which procedures, equipment, facilities, and other components serve to support human capabilities and compensate for human limitations; sometimes also called “user-centered.”

Human Factors. A multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to equipment, systems, facilities, procedures, jobs, operations, environments, training, staffing, and personnel management for safe, comfortable, efficient and effective human performance.

Human-System Integration. The concepts and processes associated with optimizing total system performance via fully incorporating human factors considerations (including staffing levels, personnel attributes and abilities, training, safety and occupational health, ergonomics, and human engineering) in program requirements, analysis, design, development, testing, implementation, and continuing support.

Incident. A near miss episode, malfunction, or failure with minor consequences that could have resulted in greater loss. An unplanned event that could have resulted in an accident, or did result in minor damage, and indicates the existence of, though may not define, a hazard or hazardous condition.

Latent Failure. A failure that is not inherently revealed at the time it occurs.

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

Maintenance. Any repair, adaptation, upgrade, or modification of National Airspace System (NAS) equipment or facilities. This includes preventive maintenance.

Mitigation. Actions taken to reduce the risk of a hazard's effects.

National Airspace System. National Airspace System: Is comprised of airspace; airports; aircraft; pilots; air navigation facilities; air traffic control (ATC) facilities; communication, surveillance, navigation, and supporting technologies and systems; operating rules, regulations, policies, and procedures; and the people who implement, sustain, or operate the system components.

NAS Change. Any change to or modification of airspace; airports; aircraft; pilots; air navigation facilities; air traffic control (ATC) facilities; communication, surveillance, navigation, and supporting technologies and systems; operating rules, regulations, policies, and procedures; and the people who implement, sustain, or operate the system components.

Oversight. To validate the development of a defined system and verify compliance to a pre-defined set of standards; Regulatory Supervision.

Physical Diversity. The separation of redundant functions such that a single point of failure does not fail both paths, which would make the service unavailable. Thus, physical diversity is another method used to increase the likelihood of service availability in the event of failures.

Process. A set of interrelated or interacting activities which transforms inputs into outputs.

Qualitative Data. Subjective data that is expressed as a measure of quality; nominal data.

Quantitative Data. Objective data expressed as a quantity, number, or amount; allows for more rational analysis and substantiation of findings.

Redundancy. System includes design attributes, which ensure duplication or repetition of elements to provide alternative functional channels in case of failure. Redundancy allows the service to be provided by more than one path to maximize the availability of the service.

Requirement. An essential attribute or characteristic of a system. It is a condition or capability that must be met or passed by a system to satisfy a contract, standard, specification, or other formally imposed document or need.

Risk. The composite of predicted severity and likelihood of the potential effect of a hazard in the worst credible system state.

(1) **Initial.** The composite of the severity and likelihood of a hazard considering only verified controls and documented assumptions for a given system state. It describes the risk at the preliminary or beginning stage of a proposed change, program or assessment.

(2) **Current.** The predicted severity and likelihood of a hazard at the current time. When determining current risk, both validated controls and verified controls may be used in the risk assessment. Current risk may change based on the actions taken by the decision-maker that relate to the validation and/or verification of the controls associated with a hazard.

(3) **Predicted Residual.** Predicted residual risk is the term used until the safety analysis is complete and all safety requirements have been verified. Predicted residual risk is based on the assumption that all safety requirements will be validated and verified.

(4) **Residual.** The risk that remains after all control techniques have been implemented or exhausted and all controls have been verified. Only verified controls can be used to assess residual risk.

Risk Acceptance. Certification by the appropriate management official that he/she understands the safety risk associated with the change and he/she accepts that safety risk into the NAS.

Risk Assumption Strategy. To accept the likelihood, probability, and consequences associated with the risk.

Risk Avoidance Strategy. To select a different approach or to not participate in the operation, procedure, or system development to avert the potential of occurrence and/or consequence.

Risk Control Strategy. To develop options and alternatives and/or take actions to minimize or eliminate the risk.

Risk Transfer Strategy. To shift the ownership of the risk to another party.

Safety. Freedom from unacceptable risk.

Safety Council. A forum for top management officials from AOV and the ATO Safety Service to meet and discuss noncompliance and other safety issues in an attempt to resolve those issues.

Safety Culture. The product of individual and group values, attitudes, competencies, and patterns of behavior that determine commitment to, and the style and proficiency of, an organization's Health and safety management. In addition, the four key components of a safety culture are reporting culture (encourage employees to divulge information about all hazards that they encounter), just culture (employees are held accountable for deliberate violations of the rules but are encouraged and rewarded for providing essential safety-related information), flexible culture (to adapt effectively to changing demands and allow quicker, smoother reactions to off-nominal events), and learning culture (willing to change based on safety indicators and hazards uncovered through assessments, data, and incidents).

Safety Directive. A mandate from AOV to ATO to take immediate corrective action to address a noncompliance issue that creates a significant unsafe condition.

Safety Management System (SMS). An integrated collection of processes, procedures, policies, and programs that are used to assess, define, and manage the safety risk in the provision of ATC and navigation services.

Safety Requirement. A control written in requirements language.

Safety Risk Management (SRM). A formalized, proactive approach to system safety. SRM is a methodology applied to all NAS changes that ensures all risks are identified and mitigated prior to the change being made. It provides a framework to ensure that once a change is made, it continues to be tracked throughout its lifecycle.

Safety Risk Management Decision Memo (SRMDM). The documentation of the decision that the proposed change does not impact NAS safety. The memo includes a written statement of the decision and supporting argument and is signed by the manager and kept on file for a period equivalent to the lifecycle of the system or change.

Safety Risk Management Document (SRMD). Thoroughly describes the safety analysis for a given proposed change. It documents the evidence to support whether or not the proposed change to the system is acceptable from a safety risk perspective. SRMDs are kept and maintained by the organization responsible for the change for a period equivalent to the lifecycle of the system or change.

Safety Risk Management Panel. A diverse group of representatives, stakeholders, and subject matter experts from the various organizations affected by the change, which conducts a

safety analysis of the proposed change and presents findings and recommendations to decision makers.

Severity. The measure of how bad the results of an event are predicted to be. Severity is determined by the worst credible outcome.

Single Point Failure. The failure of an item that would result in the failure of the system and is not compensated for by redundancy or an alternative operational procedure.

Source (of a hazard). Any potential origin of system failure, including equipment, operating environment, human factors, human-machine interface, procedures, and external services.

SRM Documentation Approval. Certification that the documentation was developed properly, hazards were systematically identified, risk was appropriately assigned, suitable mitigations were proposed, and a sound implementation and monitoring plan was prepared. SRM documentation approval does not constitute acceptance of the risk associated with the change or approval to implement the change.

Stakeholder. A group or individual that is affected by or is in some way accountable for the outcome of an undertaking; an interested party having a right, share or claim in a product or service, or in its success in possessing qualities that meet that party's needs and/or expectations.

System. An integrated set of constituent pieces that are combined in an operational or support environment to accomplish a defined objective. These pieces include people, equipment, information, procedures, facilities, services, and other support services.

System Engineering. A discipline that concentrates on the design and application of the whole (system) as distinct from the parts. It requires examining a problem in its entirety, taking into account all the facets and variables and relating the social to the technical aspect. The translation of operational requirements into design, development, implementation concepts, and requirements in the lifecycle of a system.

System State. An expression of the various conditions, characterized by quantities or qualities, in which a system can exist.

Validation. The process of proving that the right system is being built, i.e., that the system requirements are unambiguous, correct, complete, and verifiable.

Verification. The process that ensures that the system requirements have been met by the design solution and the system is ready to be used in the operational environment for which it is intended.

Worst Credible Outcome. The most unfavorable, yet believable and possible, condition given the system state.

Appendix B – Acronyms/Abbreviations

AAI - Office of Accident Investigation

AFS - Flight Standards Service

AIDS - Accident/Incident Data System

AMS - Acquisition Management System

AOV - Air Traffic Safety Oversight Service

ARP - Airports

ARTCC - Air Route Traffic Control Center

ASAP - Aviation Safety Action Program

ASIAS - Aviation Safety Information Analysis and Sharing System

ASE - Altimetry System Error

ASRP - Aviation Safety Reporting Program

ASRS - Aviation Safety Reporting System

ATC - Air Traffic Control

ATM - Air Traffic Manager

ATO - Air Traffic Organization

ATO-SG - ATO Safety Guidance

ATS - Air Traffic Service

AVS - Aviation Safety

CAA - Civil Aviation Authority

CAP - Corrective Action Plan

C-ARTS - Common Automated Radar Terminal System

CERAP - Combined Center Radar Approach Control

CFIT - Controlled Flight into Terrain

CFR - Code of Federal Regulations

CNS - Communications, Navigation, Surveillance

COO - Chief Operating Officer

CSA - Comparative Safety Assessment

CSI - Critical Safety Initiatives

CTA - Cognitive Task Analysis

DBRITE - Digital Bright Radar Indicator Tower Equipment

DoD - Department of Defense

DP - Departure Procedures

ERAM - En Route Automation Modernization

ETBA - Energy Trace and Barrier Analysis

ETMS - Enhanced Traffic Management System

FAA - Federal Aviation Administration

FAALC - FAA Logistics Center

FARs - Federal Aviation Regulations

FAST - FAA Acquisition System Toolset

FHA - Fault Hazard Analysis

FL - Flight Level

FMEA - Failure Mode and Effect Analysis

FMECA - Failure Modes, Effects, and Criticality Analysis

FMS - Flight Management System

FPC - Flow Process Charts

FRDF - Facility Reference Data File

FSAS - Facility Safety Assessment System

FSDO - Flight Standards District Office

FTA - Fault Tree Analysis

GAIN - Global Aviation Information Network

GPS - Global Positioning System

HAZOP - Hazard and Operability Tool

HEA - Human Error Analysis

HESRA - Human Error and Safety Risk Analysis

HTS - Hazard Tracking System

IAPA - Instrument Approach Procedures Automation

ICAO - International Civil Aviation Organization

IFR - Instrument Flight Rules

ILS - Instrument Landing System

INA - Integrated NASTEP Application

IOC - Initial Operating Capability

IOT&E - Independent Operational Test and Evaluation

ISD - In-Service Decision

ISR - In-Service Review

JHA - Job Hazard Analysis

JSA - Job Safety Analysis

JTA - Job Task Analyses

LAHSO - Land and Hold Short Operations

LDR - Labor Distribution Reporting

LHD - Large Height Deviation

LOB - Line of Business

LOC - Letter of Correction

LOI - Letter of Investigation

MAC - Mid-air Collision

MEL - Minimum Equipment List

MLS - Microwave Landing System

MMS - Maintenance Management System

MORT - Management Oversight and Risk Tree

NAIMS - National Airspace Incident Monitoring System

NAS - National Airspace System

NASA - National Aeronautics and Space Administration

NASTEP - NAS Technical Evaluation Program

NAT - North Atlantic

NAVAID - Navigational Aid

NCF – Non-conforming Finding

NCP - NAS Change Proposal

NFDC - National Flight Data Center

NFPO - National Flight Procedures Office

NMAC - Near Midair Collision

NMACS - Near Midair Collision System

NOCC - National Operations Control Center

NOTAM - Notice to Airmen

NTSB - National Transportation Safety Board

OA - Operations Analysis

OE - Operational Error

OEDS - Operational Error and Deviation System

OFI - Opportunity for Improvement

OI - Operational Improvements

OPI - Office of Primary Interest

ORM - Operational Risk Management

OSA - Operational Safety Assessment

OSD - Operational Sequence Diagram

OSHA - Occupational Safety and Health Administration

PAC - Pacific

PDS - Pilot Deviation System

PE - Physical Examination

PHA - Preliminary Hazard Analysis

PHL - Preliminary Hazard List

PLC - Programmable Logic Controller

PM - Preventative Maintenance

POC - Point of Contact

POS – Positive Observation

PS&J - Power Supply and Junction Box

RGCSP - Review of General Concept of Separation Panel

RI - Runway Incursion

RIS - Regulatory Information System

RNP RNAV - Required Navigation Performance for Area Navigation

RVSM - Reduced Vertical Separation Minimum

SID - Standard Instrument Departure

SME - Subject Matter Expert

SMS - Safety Management System

SOC – Safety Oversight Circular

SOIA - Simultaneous Offset Instrument Approach

SOWG - Safety Operational Working Group

SRM - Safety Risk Management

SRMD - Safety Risk Management Document

SRMDM - Safety Risk Management Decision Memo

SRMGSA - Safety Risk Management Guidance for System Acquisitions

SRMIT - Safety Risk Management Implementation Team

SSAR - System Safety Assessment Report

SSH - System Safety Handbook

SSWG - System Safety Working Group

STARS - Standard Terminal Automation Replacement System

TAA - Terminal Arrival Area

TERPS - Terminal Instrument Procedures

THA - Task Hazard Analysis

TLS - Target Level of Safety

UCR - Unsatisfactory Condition Report

VFR - Visual Flight Rules

VSM - Vertical Separation Minimum

WATRS - West Atlantic Route Structure

ZNY - New York ARTCC

Appendix C – ATO Safety Guidance Process

The ATO Safety Guidance (ATO-SG), also called ATO Safety Interim Guidance, was developed to provide new and revised SMS guidance pertaining in concurrence with the draft ATO Order, *ATO Safety Guidance*, to the ATO. ATO-SGs supplement existing orders, directives, guidance, and materials, including ATO Order JO 1000.37, *Air Traffic Organization Safety Management System,* and this manual.

Information and guidance contained in ATO-SGs are included in existing orders, directives, and materials as they undergo scheduled updates. As ATO-SGs are incorporated into permanent materials, they are removed from distribution. The ATO announces newly posted ATO-SGs by e-mail to Safety Directors, Safety Managers, and Safety Engineers at FAA headquarters, for further dissemination within their respective organizations. In addition, ATO-SGs are posted on the SMS Directorate section of the ATO Experience web site within five business days.

ATO-SGs contain guidance regarding the processes and procedures applicable to the safety of the NAS. An ATO-SG may provide information alone or may provide a combination of information and guidance material or recommended actions ATO personnel should take to meet the requirements of directives and orders. The ATO-SG process is depicted on the following page.

ATO Safety Guidance Process

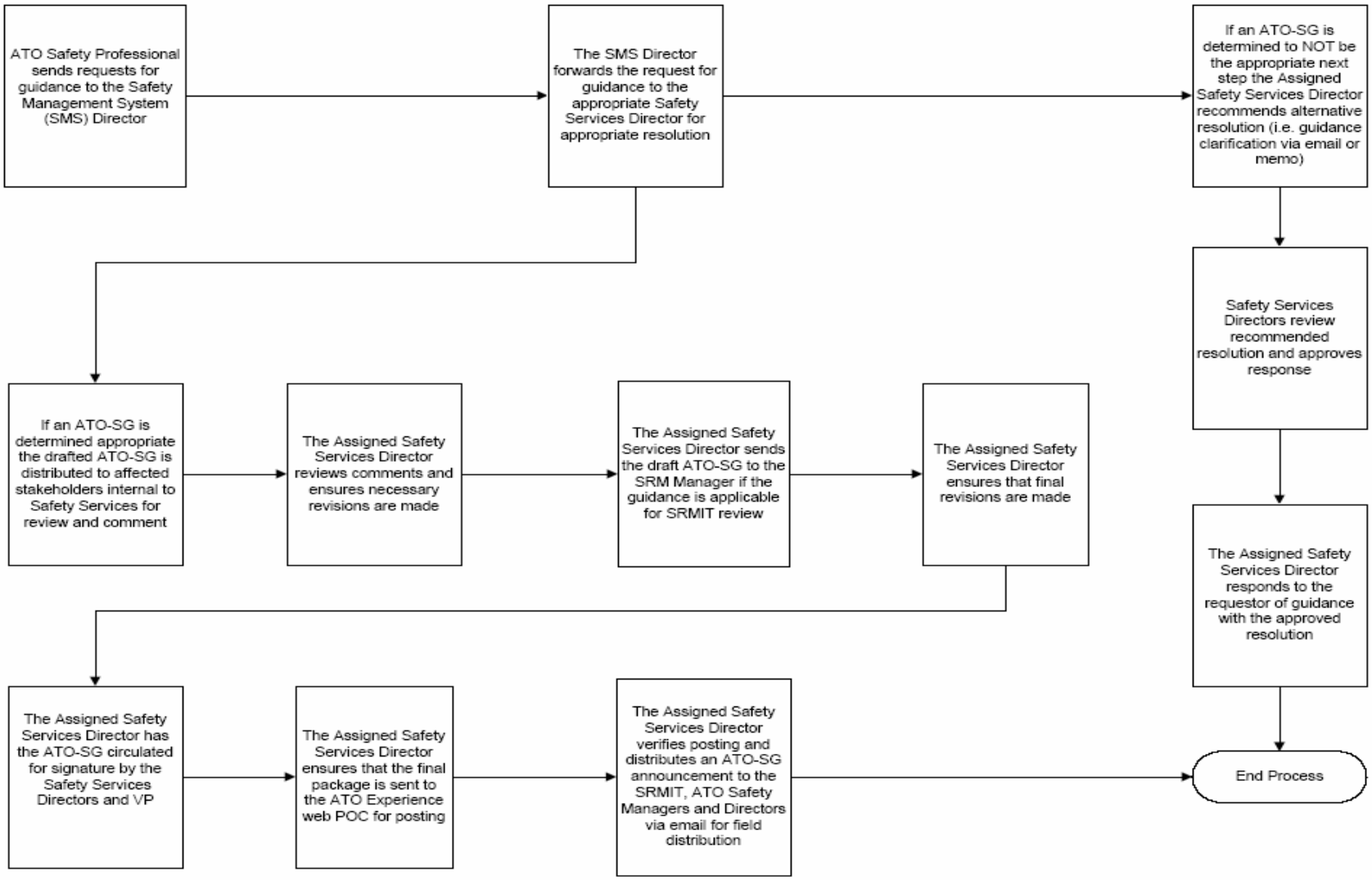


Figure C.1: ATO Safety Guidance Process Flow

Appendix D – FAA Documents Related to SMS Requirements

The following documents (orders, directives, regulations, handbooks, and manuals) address NAS safety management and are related to the processes described in this manual. Note that this list is not all-inclusive and represents a small portion of FAA documents that pertain to safety management.

Some documents listed below may have been updated since this list was compiled. Refer to the Office of Primary Interest (OPI) for the most recent version of the document.

General:

- Order 1220.2, *FAA Procedures for Handling NTSB Safety Recommendations*
- Order 1800.6, *Unsatisfactory Condition Report RIS*
- Advisory Circular No: 00-46: *Aviation Safety Reporting Program (ASRP)*
- Order 1100.161, *Air Traffic Safety Oversight*
- Order 8000.86, *Air Traffic Safety Oversight Compliance Process*
- Order 8000.73, *Aviation Safety Hotline*
- Order 9550.8, *Human Factors Policy*
- HF-STD-001, *Human Factors Design Standard*
- DOT/FAA/AR-03/69, *FAA Human Factors Acquisition Job Aid*

Airports:

- 14 CFR: Part 77 - *Objects Affecting Navigable Airspace*
- 14 CFR: Part 157 - *Notice of construction, alteration, activation and deactivation of airports*
- 14 CFR: Part 139 - *Certification and operations: Land airports serving certain air carriers*
- Order 5010.4, *Airport Safety Data Program*

Air Traffic Control:

- Advisory Circular 120-66, *Aviation Safety Action Program (ASAP)*
- Notice JO 7210.663, *Operational Error Reporting, Investigation, and Severity Policies* Order 1100.2, *Organization – FAA Headquarters*
- Order 1800.3B, *National Flight Standards Work Program Guidelines*
- Order 1800.14, *Airway Facilities Evaluation Program*
- Order 1800.66, *Configuration Management Policy*
- Order 3120.4, *Air Traffic Technical Training*
- Order 3120.27, *Performance Verification for En Route and Terminal Initial Qualification Training*
- Order 6040.15, *National Airspace Performance Reporting System*
- Order 6050.19, *Radio Spectrum Planning*
- Order 6050.22, *Radio Frequency Interference Investigation and Reporting*
- Order 6050.32, *Spectrum Management Regulations and Procedures Manual*
- Order 6480.4, *Airport Traffic Control Tower Siting Criteria*
- Order 7010.1, *Air Traffic Evaluations*
- Order 7050.1, *Runway Safety Program*
- Order 7110.1S, *Air Traffic Control Safety Evaluations and Audits*

- Order 7110.49, *Unlawful Interference – Hijack/Bomb (Threat) Aboard Aircraft Procedures and Covert Signals*
- Order 7110.65, *Air Traffic Control*
- Order 7110.82, *Monitoring of Navigation, Longitudinal Separation and Altitude Keeping Performance in Oceanic Airspace*
- Order 7110.112, *Simultaneous ILS/MLS Blunder Data Collection*
- Order 7210.3, *Facility Operation and Administration*
- Order 7210.56, *Air Traffic Quality Assurance*
- Order 7220.1, *Certification and Rating Procedures*
- Order 7400.2, *Procedures for Handling Airspace Matters*
- Order 7450.1, *Special Use Airspace Management System*
- Order 7610.4, *Special Military Operations*
- Order AF 7900.5A Change 2, *Publication of National Airspace Publication of National Airspace System Information*
- Order 7900.2, *Reporting of Electronic Navigation Aids and Communication Facilities Data to the NFDC*
- Order 7910.3, *Position Display Map Program*
- Order 7930.2, *Notices to Airmen (NOTAMs)*
- Order 8020.16, *Air Traffic Organization Aircraft Accident and Incident Notification, Investigation, and Reporting*

Facilities and Equipment:

- Order 1320.58, *Instructions for Writing Notices, Maintenance Technical Handbooks, and System Support Directives*
- Order 1800.66, *Configuration Management Policy*
- Order 1900.47, *Air Traffic Services Contingency Plan*
- Order 3000.10, *Airway Facilities Technical Training Program*
- Order 3400.3, *Airway Facilities Maintenance Personnel Certification Program*
- Order 3900.19, *Occupational Safety and Health Program*
- Order 4140.1, *Integrated Material Management Program*
- Order 4441.16, *Acquisition of Telecommunications Systems, Equipment and Services*
- Order 4630.5, *Quality and Reliability Assurance of General Operating Materiel Managed by the FAA Logistics Center (FAALC)*
- Order AF 6000.10, *Airway Facilities Service Maintenance Program*
- Order 6000.54, *Airway Facilities Hazard Communication Program*
- Order 6000.15, *General Maintenance Handbook for National Airspace System (NAS) Facilities*
- Order 6000.30, *National Airspace System Maintenance Policy*
- Order 6000.46, *Maintenance Management System (MMS) Software Operations and Management*
- Order 6000.48, *General Maintenance Logging Handbook*
- Order 6000.50, *Airway Facilities National Airspace System Operations Procedures*
- Order 6000.53, *Remote Maintenance Monitoring Interfaces*
- Order 6030.31, *Restoration of Operational Facilities*
- Order 6030.41, *Notification Plan for Unscheduled Facility and Service Interruptions and Other Significant Events*

- Order 6032.1, *National Airspace System Modification Program*
- Order 6040.6, *Airway Facilities NAS Technical Evaluation Program*
- Order 6040.15, *National Airspace Performance Reporting System*
- Order 6300.13, *Radar Systems Optimization and Flight Inspection Handbook*
- Order 7900.4, *Reporting of Military-Certified Air Navigation Facilities to the NFDC (RIS: AT 7900-20)*
- Order 7920.1, *Content Criteria for Airman's Information Publications Originating in the NFDC*

Flight Procedure/Flight Inspection:

- Order VN 3330.2, *National Flight Procedures Office (NFPO) Certification Program for Procedures Personnel*
- Order VN 4040.3, *Flight Inspection Proficiency, Standardization Evaluation Program*
- Order 4040.24, *FAA Flight Program Responsibilities and Operational Standards for FAA Aircraft*
- Order 8200.1, *United States Standard Flight Inspection Manual*
- Order VN 8240.3, *Certification of Flight Inspection Personnel*
- Order 8240.36, *Instructions for Flight Inspection Reporting*
- Order 8260.3, *United States Standard for Terminal Instrument Procedures (TERPS)*
- *Order VN 8260.4, ILS Obstacle Risk Analysis*
- Order 8260.15, *United States Army Terminal Instrument Procedures Service*
- Order 8260.16, *Airport Obstruction Surveys*
- Order 8260.19, *Flight Procedures and Airspace*
- Order 8260.23, *Calculation of Radio Altimeter Height*
- Order 8260.26, *Establishing and Scheduling Standard Instrument Procedure Effective Dates*
- Order 8260.31, *Foreign Terminal Instrument Procedures*
- Order 8260.32, *U.S. Air Force Terminal Instrument Procedures Service*
- Order 8260.33, *Instrument Approach Procedures Automation (IAPA) Program*
- Order 8260.37, *Heliport Civil Utilization of Collocated Microwave Landing System (MLS)*
- Order 8260.38, *Civil Utilization of Global Positioning System (GPS)*
- Order 8260.40, *Flight Management System (FMS) Instrument Procedures Development*
- Order 8260.42, *Helicopter Global Positioning System (GPS) Nonprecision Approach Criteria*
- Order 8260.43, *Flight Procedures Management Program*
- Order 8260.44, *Civil Utilization of Area Navigation (RNAV) Departure Procedures*
- Order 8260.45, *Terminal Arrival Area (TAA) Design Criteria*
- Order 8260.46, *Departure Procedures (DP) Program*
- Order 8260.48, *Area Navigation (RNAV) Approach Construction Criteria*

New Systems:

- Order 4400.57, *System for Acquisition Management*
- Federal Aviation Administration Acquisition Management System
- Safety Risk Management Guidance for System Acquisitions (SRMGSA)
- System Engineering Manual (SEM)
- IOT&E Operations Manual, July 2005, Version 12 CHG 2

- NAS-SR-1000 Revision A, National Airspace System System Requirements Specifications (Functional View)

Safety Management Systems:

- FAA Advisory Circular 25.1309, *System Design Analysis*
- Order 8000.365, *Safety Oversight Circulars (SOC)*
- Order 8040.4, *Safety Risk Management*
- FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*
- FAA Order JO 1000.39, *Air Traffic Organization, En Route and Oceanic Services, Safety Management System*
- FAA Order 1100.161, *Air Traffic Safety Oversight*
- FAA Order 7010.1S, *Air Traffic Control Safety Evaluations and Audits*
- FAA Order 7000.7, *Air Traffic Organization Terminal Services Safety Management System Program*
- FAA Order JW 7232.15, *Air Traffic Organization Western Terminal Service Area Safety Risk Management Implementation*
- FAA Order JE 7232.14, *Air Traffic Organization Eastern Terminal Service Area Safety Risk Management Implementation*

Appendix E – SRMDM Template

Federal Aviation Administration

Memorandum

Date:

To: < A designated management official from the affected Service Unit(s) >

From: < Manager, ATO-X, Facility Y or Organization >

Prepared by: < Name >

Subject: Safety Risk Management Decision Memorandum (SRMDM) for < name of proposed change/case file >

National Airspace System (NAS) Change:
< Provide a brief reasoning/motivation for the change/procedure initiative. Include the scope of the change (local or NAS-wide) and specific reasons for proposing the change (e.g., increased airport capacity, operational efficiency, reduction in operating costs, etc.). >

Rationale for not Requiring further SRM Analysis:
< In this paragraph, state the reason(s) as to why further SRM analysis is not required for the proposed change. You must include or attach all supporting documentation used in the decision process which determined the change does NOT introduce any safety risk into the NAS. Additionally, you must ensure with supporting rationale that your reason for not performing further SRM analysis is in compliance with the Safety Management System (SMS) Manual. The decision memo must be kept on file for a period equivalent to the lifecycle of the system or the change.>

<If the proposed change affects other organizations, you are responsible for coordinating the proposal of the change and the decision to not perform additional SRM. In this paragraph you need to have a statement of coordination (e.g., ATO-X, Y and Z have all reviewed and concur that the proposed change does not introduce any safety risk into the NAS). >

We, the undersigned, assure that the change described above does not introduce any safety risk into the NAS.

< NOTE: The signature blocks below represent the minimum signature requirement for an SRMDM that does not require the concurrence of the ATO SSWG Chairman. SRMDMs reviewed by the ATO SSWG require additional signature blocks; refer to the SRMDM guidance in the SMS Manual for requirements. >

Signature(s):

*Submitted by:**

_____	_____	_____
Signature	Name & Organization	Date

Concurred by:

_____	_____	_____
Signature	Name & Organization	Date

***** *The change proponent may meet the "Submitted by" signature requirement by initialing the "from" line of the SRMDM (contact your Service Unit's Safety Engineer for Service Unit specific guidance).*

File: Administrative
WP: Draft SRM Decision Memo.doc
ATO-S:<TBD>, <Name>:<TBD>:5-4811<Date>

Appendix F – SRMDM Review Checklist

SRMDM Title: _____ SRMD Identifier: _____

Name of Originator: _____

Originating Organization: _____ Date Received by ATO-S: _____

Assigned to: _____

No.	SMS Manual Requirement	SMS Reference	Compliance	Category	Remarks
1	Is the document clearly titled?	Appendix E	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
2	Is the document appropriately dated?	Appendix E	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
3	Is the originator appropriately identified?	Appendix E	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
4	Did the appropriate individuals approve the document?	3.5.2	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
5	Is this a change to a separation standard or periodicity of maintenance?	3.4.5	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
6	Is the change clearly described?	3.5.2 and Appendix E	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
7	Were stakeholders appropriately involved/ consulted?	3.4	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	

No.	SMS Manual Requirement	SMS Reference	Compliance	Category	Remarks
8	Was the correct level of safety analysis appropriately identified?	3.5	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
9	Is there clear justification/ rationale for the SRM decision?	3.5.2	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	

Appendix G – Hazard Identification and Analysis Tools and Techniques

The descriptions in this appendix are designed to provide additional information regarding the selection of hazard identification and analysis tools and techniques described in Table 3.1 (Section 3.8.6).

PRELIMINARY HAZARD ANALYSIS

FORMAL NAME: Preliminary Hazard Analysis (PHA)

ALTERNATIVE NAMES: None

PURPOSE: To provide an initial overview of the hazards present in the overall flow of the operation. It provides a hazard assessment that is broad, but usually not deep. The key idea of the PHA is to consider all of the hazards inherent to each aspect of an operation, without regard to risk. The PHA helps overcome the tendency to focus immediately on risk in one aspect of an operation, sometimes at the expense of overlooking more serious issues elsewhere in the operation. The PHA will often serve as the hazard identification process when risk is low or routine. In higher risk operations, it serves to focus and prioritize follow-on hazard analyses by displaying the full range of risk issues.

APPLICATION: Personnel use the PHA in nearly all risk management applications except the most time-critical. Its broad scope is an excellent guide to the identification of issues that may require more detailed hazard identification tools.

METHOD: The PHA is usually based on the Operations Analysis, also known as a Flow Diagram, taking each event in turn from it. Analysts apply their experience and intuition, use reference publications and standards of various kinds, and consult with personnel who may have useful input. Resource and time limitations, as well as the estimate of the degree of overall risk inherent in the operation, dictate the extent of the effort. Analysts often list the hazards that they detect directly on a copy of the Operations Analysis. Alternatively, analysts can use a more formal PHA format such as the worksheet shown in the following example. They use the completed PHA to identify hazards requiring more in-depth hazard identification. Key to the effectiveness of the PHA is ensuring that personnel address all events of the operation.

When using the PHA, analysts should:

- Ensure adequate space on the worksheet between each event to allow several hazards to be noted for each event
- List the hazards noted for each operational phase
- Strive for detail within the time limits

A copy of a PHA accomplished for an earlier similar operation would aid in the process.

COMMENTS: The PHA is relatively easy to use and takes little time. Its significance in impacting risk comes from the forced consideration of risk in all events of an operation. This means that a key to success is to link the PHA closely to the Operations Analysis.

EXAMPLE: The following is an example of a PHA.

Hazard # (1)	Hazard Description (2)	Causes (3)	System State (4)	Existing Control or Requirement (5)	Possible Effect (6)	Severity/ Rationale (7)	Likelihood/ Rationale (8)	Current/ Initial Risk (9)	Recommended Safety Requirements (10)	Predicted Residual Risk (11)
1	Loss of control of 8 PLC touch screen in tower cab. User cannot control XYZ System at critical time.	Loss of control occurs due to: Hardware failure/ malfunction Software failure/ malfunction Human error Electrical short occurs; Loss of all power	System maintenance occurring during the operation Aircraft on final approach under adverse visual conditions	1. Training shall be provided to ATC for contingency procedures to ensure situational awareness while using XYZ System. 2. Pilot shall raise the minimum approach, in accordance with the operational specification according to approach procedures as designated in the Airport (specific) Approach Chart(s). 3. XYZ System shall comply with FAA requirements for critical and essential power (SR-1000 XYZ System Requirement Specifications 3.7.4. Facilities). 4. ATCT shall use 7110.65 procedures for validating aircraft ID, position, and altitude. 5. Pilot shall follow FAR 91.175, FAR 91.185, FAR 97, and FAR 91.3 as applicable for loss of runway lighting dependent on type and phase of approach to landing aircraft. 6. The XYZ System shall comply with reliability and availability requirements of NAS-SR-1000, paragraph 3.8.1 for failures, XYZ System anomalies, and malfunctions, in critical, essential, and routine services. 7. A redundant touch screen shall be provided in tower c	Temporary loss of function	4 Minor due to a slight reduction in safety margin	C Remote expected to occur xx often based on subject matter expertise and/or operational data	4C	1. XYZ System shall incorporate XYZ System failure and health monitoring to ensure that XYZ System failures/ malfunctions are detected and reported automatically. 2. XYZ System software shall comply with DO 278 or similar best practice. 3. XYZ System shall comply with FAA-STD-G-2100G (Specifications for Electronic Equipment, General Requirements) or equivalent commercial standards. 4. Training shall be provided to Airway Facilities (AF) on appropriate performance of all corrective and preventative maintenance procedures associated with XYZ System. 5. Human/machine interface(s) shall meet requirements in FAA Visual Requirements for Ground Display XYZ Systems, Version 1.1. 6. XYZ System Program Management shall provide logistical support for the immediate availability for all space parts including hardware, software, and firmware related to XYZ System.	4D

OPERATIONAL SAFETY ASSESSMENT

FORMAL NAME: Operational Safety Assessment (OSA)

ALTERNATIVE NAMES: None

PURPOSE: To provide a systems engineering practice of developing coordinated, systematic safety objectives and requirements for the overall system (including procedural considerations) early in the development phase. The OSA is a development tool based on the assessment of hazard severity. It also establishes how safety requirements are to be allocated between air and ground components and how performance and interoperability requirements might be influenced. A full description and instructions on how to perform an OSA are in the Acquisition Management System (AMS) FAA Acquisition System Toolset (FAST).

METHOD: The OSA is completed during the Concept and Requirements Definition (CRD) phase and is completed and approved prior to the JRC Secretariat's cut-off date for the Investment Analysis Readiness Decision (IARD). OSA requirements are included in the initial Requirements Document (iRD). The OSA is composed of three sections:

1. 1. Operational Services Environment Description (OSED)
2. 2. Operational Hazard Assessment (OHA)
3. 3. Allocation of Safety Objectives and Requirements (ASOR) List

The OSED is a description of the system's physical and functional characteristics, the environment's physical and functional characteristics, and air traffic services and Operational procedures. It includes both air and ground elements of the system analyzed.

The OHA is a qualitative severity assessment of the hazards associated with the system described in the OSED. The OHA includes work sheets and the preliminary hazard list.

The ASOR is a process of using hazard severity to determine the objectives (target level of safety) and requirements of the system. There are two levels of requirements in this process: (1) objectives (or goals) and (2) requirements (or minimum levels of acceptable performance). Its purpose is to establish requirements that ensure the probability of a hazard leading to an accident has an inverse relationship to the accident's severity or consequence.

Program Office personnel conduct the OSA with the guidance and assistance of the ATO SSWG. The OSA analysis is documented in an SRMD and submitted to the ATO SSWG for review. The results of the OSA are briefed at the JRC if it was a factor in selecting the chosen option.

EXAMPLE: The following provides an example of an OHA. Information on preparing an OSA and examples of an OSED and ASOR list are provided on the Safety Services ATO Experience Site.

.

Operational Hazard Assessment (OHA) Hazard Description Tabular Worksheet

OHA Worksheets

Operational Objective/ Intention Capability:	1 Provide preflight functions.				
A Air Traffic Service	B Operational Hazard	C Operating phase - System State	D Effect of Operational Hazard	E Operational Hazard Severity Classification	F Recommended Requirements
1.1 Provide weather and aeronautical information to pilots prior to departure	1.1.1 Weather information is unavailable	Preflight	Pilot may make an improper GO/NO GO decision and experience delays and/or encounter severe, adverse weather conditions resulting in fatalities and/or loss of aircraft.	Hazardous	SOR 4
	1.1.2 Weather information is erroneous	Preflight	Pilot may make an improper GO/NO GO decision and experience delays and/or encounter severe, adverse weather conditions resulting in fatalities and/or loss of aircraft.	Hazardous	SOR 5
	1.1.3 Aeronautical Information, e.g. NOTAMs, is unavailable	Preflight	Pilot may make an improper GO/NO GO decision based upon lack of data and encounter delays and/or unsafe in-flight or landing conditions which result in fatalities and/or loss of aircraft.	Hazardous	SOR 6
	1.1.4 Aeronautical Information, e.g. NOTAMs, is erroneous	Preflight	Pilot may make an improper GO/NO GO decision based upon erroneous data and encounter delays and/or unsafe in-flight or landing conditions which result in fatalities and/or loss of aircraft.	Hazardous	SOR 7
	1.1.5 SUA information is unavailable	Preflight	Pilot may make an improper GO/NO GO decision and encounter delays and/or unsafe in-flight or landing conditions which result in fatalities and/or loss of aircraft.	Hazardous	SOR 8
	1.1.6 SUA information is erroneous	Preflight	Pilot may make an improper GO/NO GO decision and encounter delays and/or unsafe in-flight or landing conditions which result in fatalities and/or loss of aircraft.	Hazardous	SOR 9

COMPARATIVE SAFETY ASSESSMENT

FORMAL NAME: Comparative Safety Assessment (CSA)

ALTERNATIVE NAMES: None

PURPOSE: To provide management with a listing of all of the hazards associated with a change, along with a risk assessment for each alternative hazard combination that is considered. It is used to rank the options for decision-making purposes. The CSA's broad scope is an excellent way to identify issues that may require more detailed hazard identification tools.

METHOD: The CSA is a risk assessment, in that it defines both severity and likelihood in terms of the current risk of the system. Whereas an OSA defines the target level of safety, a risk assessment provides an estimation of the risk associated with the identified hazards.

The first step within the CSA process involves describing the system under study in terms of the 5M model. Since most decisions are a selection of alternatives, each alternative must be described in sufficient detail to ensure the audience can understand the hazards and risks evaluated. Many times one of the alternatives will be "no change," or retaining the baseline system. A preliminary hazard list (PHL) is developed and then 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. A CSA should be written so that the decision-maker can clearly distinguish the relative safety merit of each alternative.

The CSA analyses are conducted in support of the Initial Investment Decision (IID) and are completed and approved prior to the JRC Secretariat's cut-off date for that decision. The basic tasks involved in the development of the CSA are depicted in Figure G.1.

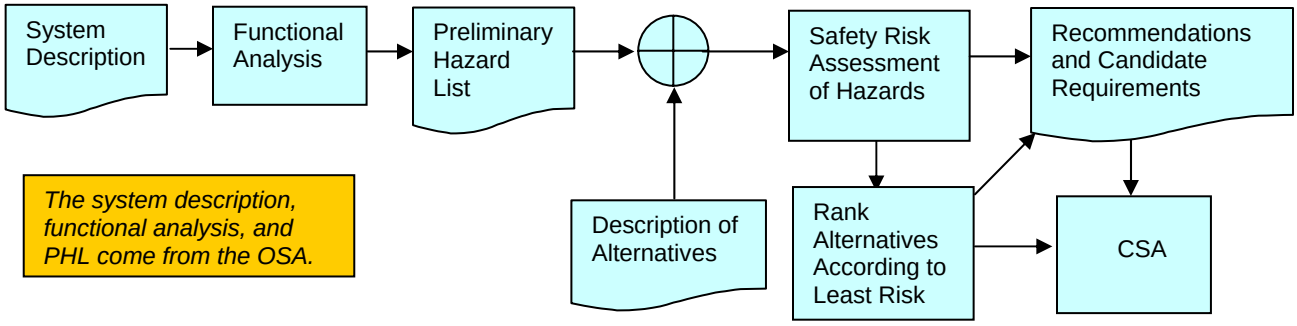


Figure G1: CSA Process Flow

The identified hazards and the risk assessments for each of the alternatives addressed throughout the Investment Analysis (IA) are documented in the Investment Analysis Report (IAR) or Business Case Analysis Report (BCAR). Any requirements recommended in the CSA that apply to the selected options are compiled in the Safety Requirements Verification Table (SRVT) and supplied to the program for inclusion in the final Requirements Document (fRD).

Program Office personnel conduct the CSA with the guidance and assistance of the ATO SSWG. The CSA is submitted to the ATO SSWG as an SRMD. The results of the CSA are briefed at the JRC if it was a factor in selecting the chosen option.

.

EXAMPLE: The following is an example of a CSA.

Comparative Safety Assessment (CSA) Hazard Description Tabular Worksheet

Hazard # (1)	Hazard Description (2)	Causes (3)	System State (4)	Possible Effect (5)	Severity/ Rationale (6)	Existing Safety Solutions (7)	Site 1A	Site 7	Site 9
1	Potential interference with navigation equipment (both planned and existing equipment) Interference with NAS equipment generates hazardously misleading information, followed by loss of situational awareness, leading to loss of separation between two moving aircraft/vehicles	Structural E3 interference from new tower location Line of Sight	During IFR / IMC operations	Interference with NAS equipment generates hazardously misleading information, followed by loss of situational awareness Loss of separation	Sites 1A, 7, and 9 5 – No Safety Effect Based on the operational expertise of the NAS watch specialist	• FAA Order 6480.4-5a (5), *The Airport Traffic Control Siting Criteria* • Radar environment • FAA Order 7400.2E, *Objects Effecting Navigable Airspace* • ATCT shall use 7110.65 procedures for validating and/or verifying aircraft ID, position, and altitude • FAR 91.63, 91.75, 91.85, 97 • Other NAVAIDS (e.g. GPS)	5E Extremely improbable due to the fact that the NAS Watch screening tool revealed no navigation interference issues at this site (verified by NAS watch study) **(Low Risk Hazard)**	5E extremely improbable due to the fact that the NAS Watch screening tool revealed no navigation interference issues at this site (verified by NAS watch study) **(Low Risk Hazard)**	5E extremely improbable due to the NAS Watch screening tool revealed no navigation interference issues at this site (verified by NAS – watch study) **(Low Risk Hazard)**
2	Potential interference with communication equipment (both planned and existing equipment)	Structural E3 interference from new tower location	During both VMC and IMC operations, including departures and approaches , up to and including CAT II, and surface procedures	Interference with NAS equipment generates loss of communication	Site 1A 3 - Major Due to the fact that there is potential communication interference of the Radio Communications Outlet/ Remote Transmitter Receiver (RCO/RTR) Sites 7 & 9 5 – No Safety Effect • Due to the fact that there is no potential impact to communication systems for Sites 7 and 9 • Based on the operational expertise of the NAS watch specialist	• FAA Order 6480.4-5a (5), *The Airport Traffic Control Siting Criteria* • Radar environment • ATCT shall use 7110.65 procedures for validating and/or verifying aircraft ID, position, and, altitude. • FAR 91.63, 91.75, 91.85, 97 • FAA Order 7400.2E, *Objects Effecting Navigable Airspace*	3C Remote due to the fact that there is a potential impact to the RCO/RTR (verified by NAS watch study) **(Medium Risk Hazard)**	5E Extremely improbable due to the fact that the NAS Watch screening tool revealed no communication interference issues (verified by NAS watch study) **(Low Risk Hazard)**	5E extremely improbable due to the NAS Watch screening tool revealed no communication interference issues at this site (verified by NAS – watch study) **(Low Risk Hazard)**

FAULT HAZARD ANALYSIS

FORMAL NAME: Fault Hazard Analysis

ALTERNATIVE NAMES: Fault/Failure Hazard Analysis

PURPOSE: To identify and evaluate component hazard modes, determine causes of these hazards, and determine resultant effects to the sub-system and its operation.

DESCRIPTION: The Fault Hazard Analysis is a deductive method of analysis that personnel can use exclusively as a qualitative analysis or, if desired, they can expand to a quantitative one. The fault hazard analysis requires a detailed investigation of the sub-systems to determine component hazard modes, causes of these hazards, and resultant effects to the sub-system and its operation. This type of analysis is a form of a family of reliability analyses called Failure Mode and Effect Analysis (FMEA)/Failure Modes, Effects, and Criticality Analysis (FMECA). The chief difference between the FMEA/FMECA and the Fault Hazard Analysis is a matter of depth. Wherein the FMEA/FMECA looks at all failures and their effects, the fault hazard analysis is charged only with consideration of those effects that are safety-related. The Fault Hazard Analysis of a sub-system is an engineering analysis that answers a series of questions:

- What can fail?
- How can it fail?
- How frequently will it fail?
- What are the effects of the failure?
- How important, from a safety viewpoint, are the effects of the failure?

FAILURE MODE AND EFFECT ANALYSIS AND FAILURE MODES, EFFECTS, AND CRITICALITY ANALYSIS

FORMAL NAME: Failure Mode and Effect Analysis (FMEA) or Failure Modes, Effects, and Criticality Analysis (FMECA)

ALTERNATIVE NAMES: None

PURPOSE: To identify component and sub-system failure modes, evaluate the results of the failure modes, determine rates and probability, and demonstrate compliance with safety requirements.

DESCRIPTION: FMECAs and FMEAs are important reliability program tools that provide data usable by the system safety professional. The performance of an FMEA is the first step in generating the FMECA. Both types of analyses can serve as a final product depending on the situation. One generates a FMECA from a FMEA by adding a criticality figure of merit. One performs these analyses for reliability, safety, and supportability information. Personnel more commonly use the FMECA version; it is more suited for hazard control. Hazard analyses typically use a top down analysis methodology (e.g., Fault Tree). The approach first identifies specific hazards and isolates all possible (or probable) causes. One may perform the FMEA/FMECA either top down or bottom up—usually the latter.

Hazard analyses consider failures, operating procedures, human errors and human-to-system interfaces, and transient conditions in the list of hazard causes. The FMECA is more limited. It only considers failures (hardware and software). One generates it from a different set of questions than the hazard analysis:

- If this fails, what is the impact on the system?
- Can I detect it?
- Will it cause anything else to fail? (If so, the induced failure is called a secondary failure.)

One may perform FMEAs at the hardware or functional level and they often are a combination of both. For economic reasons, personnel often perform the FMEA at the functional level below the printed circuit board or software module assembly level and at hardware or smaller code groups at higher assembly levels. The approach is designed to characterize the results of all probable component failure modes or every low level function.

WHAT-IF ANALYSIS

FORMAL NAME: What-If Analysis

ALTERNATIVE NAMES: "What If" Technique

PURPOSE: To identify hazards. The What-If Analysis is one of the most powerful hazard identification techniques. As in the case of the Scenario Analysis (see page G-12), it is designed to add structure to the intuitive and experiential expertise of operational personnel. The What-If Analysis is especially effective in capturing hazard data about failure modes that may create hazards. It is somewhat more structured than the Preliminary Hazard Analysis (PHA). Because of its ease of use, it is probably the single most practical and effective technique for use by operational personnel.

APPLICATION: Personnel should use the What-If Analysis in most hazard identification applications, including many time-critical applications. A classic use of the What-If Analysis is as the first technique one uses after the Operations Analysis (OA) and the PHA. For example, the PHA reveals an area of hazard that needs additional investigation. The best single technique to further investigate that area will be the What-If Analysis. The user will zoom in on the particular area of concern and then use the What-If Analysis to identify the hazards.

METHOD: Ensure that participants have a thorough knowledge of the anticipated flow of the operation. Visualize the expected flow of events in time sequence from the beginning to the end of the operation following these steps:

- Select a segment of the operation on which to focus
- Visualize the selected segment with "Murphy" injected
- Make a conscious effort to visualize hazards
- Ask "what if various failures occurred or problems arose?"
- Add hazards and their causes to your hazard list and assess them based on probability and severity

One can expand the What-If Analysis to further explore the hazards in an operation by developing short scenarios that reflect the worst credible outcome from the compound effects of multiple hazards in the operation. Follow these guidelines in writing scenarios:

- Target length is five or six sentences, 60 words
- Do not dwell on grammatical details
- Include elements of Mission, (hu)Man, Machine, Management, and Media
- Start with history
- Encourage imagination and intuition
- Carry the scenario to the worst credible outcome
- Use a single person or group to edit

EXAMPLE: The following is an extract from the typical output from the What-If Analysis.

Situation: Picture a group of three operational employees informally applying the round robin procedure for the What-If Analysis to a task to move a multi-ton machine from one location to another. A part of the discussion might go as follows:
Joe: What if the machine tips over and falls breaking the electrical wires that run within the walls behind it? Bill: What if it strikes the welding manifolds located on the wall on the West Side? (This illustrates “piggybacking” as Bill produces a variation of the hazard initially presented by Joe.) Mary: What if the floor fails due to the concentration of weight on the base of the lifting device? Joe: What if the point on the machine used to lift it is damaged by the lift? Bill: What if there are electrical, air pressure hoses, or other attachments to the machine that are not properly neutralized? Mary: What if the lock out/tag out is not properly applied to energy sources servicing the machine? And so on....
Note: The group might break down the list above as follows: Group 1: Machine falling hazards Group 2: Weight induced failures Group 3: Machine disconnect and preparation hazards The group then subjects these related groups of hazards to the remaining five steps of the Operational Risk Management (ORM) process.

SCENARIO ANALYSIS

FORMAL NAME: Scenario Analysis

ALTERNATIVE NAMES: Scenario Process Technique, Mental Movie Technique

PURPOSE: To identify hazards by visualizing them. It is designed to capture the intuitive and experiential expertise of personnel involved in planning or executing an operation in a structured manner. It is especially useful in connecting individual hazards into situations that might actually occur. It is also used to visualize the worst credible outcome of one or more related hazards and, is therefore, an important contributor to the risk assessment process.

APPLICATION: Personnel should use the Scenario Analysis in most hazard identification applications, including some time-critical applications. In the time-critical mode, it is indeed one of the few practical techniques, in that the user can quickly form a "mental movie" of the flow of events immediately ahead and the associated hazards.

METHOD: The user of the Scenario Analysis attempts to visualize the flow of events in an operation. This is often described as constructing a "mental movie." Usually, the best procedure is to use the flow of events established in the Operations Analysis (OA). An effective method is to visualize the flow of events twice. The first time, see the events as they are intended to flow. The next time, inject "Murphy" at every possible turn. As hazards are visualized, they are recorded for further action. Some guidelines for the development of scenarios are as follows:

- Limit them to 60 words or less
- Do not get tied up in grammatical excellence (in fact they don't have to be recorded at all)
- Use historical experience but avoid embarrassing anyone
- Encourage imagination (this helps identify risks that have not been previously encountered)
- Carry scenarios to the worst credible event

EXAMPLE: The following is an example of the Scenario Analysis using the Machine Movement Scenario.

FROM MACHINE MOVEMENT EXAMPLE: As the machine was being jacked-up to permit placement of the forklift, the fitting that was the lift point on the machine broke. The machine tilted in that direction and fell over striking the nearby wall. This in turn, broke a fuel gas line in the wall. The gas was turned off as a precaution, but the blow to the metal line caused the valve to which it was attached to break, releasing gas into the atmosphere. The gas quickly reached the motor of a nearby fan (not explosion proof) and a small explosion followed. Several personnel were badly burned and that entire section of the shop was badly damaged. The shop was out of action for three weeks.

CHANGE ANALYSIS

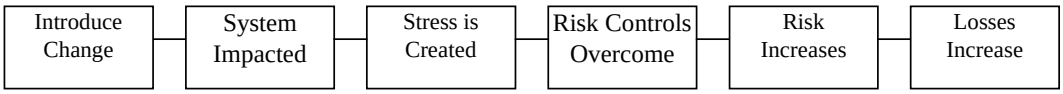
FORMAL NAME: Change Analysis

ALTERNATIVE NAMES: None

PURPOSE: To analyze the hazard implications of either planned or incremental changes. Change is an important source of risk in operational processes.

The following figure illustrates this causal relationship.

Change Causation



Some changes are planned, but many others occur incrementally over time without any conscious direction. Personnel use the Change Analysis to analyze the hazard implications of either planned or incremental changes. The Change Analysis helps to focus only on the changed aspects of the operation, thus eliminating the need to reanalyze the total operation simply because a change has occurred in one area. Personnel also use the Change Analysis to detect the occurrence of change. By periodically comparing current procedures with previous ones, they identify and clearly define unplanned changes. Finally, Change Analysis is an important accident investigation tool. Because many incidents/accidents are due to the injection of change into systems, an important investigative objective is to identify these changes using the Change Analysis procedure.

APPLICATION: Personnel should routinely use the Change Analysis in the following situations:

- Whenever changes are planned in operations in which there is significant operational risk of any kind (e.g., the decision to conduct a certain type of operation at night that has heretofore only been done in daylight)
- Periodically in any critical operation, to detect the occurrence of unplanned changes
- As an accident investigation tool

As the only hazard identification tool required when an operational area has been subjected to in-depth hazard analysis, the Change Analysis will reveal whether any elements exist in the current operations that were not considered in the previous in-depth analysis.

METHOD: The Change Analysis is best accomplished using a format such as the sample worksheet that follows. The factors in the column on the left side of this tool are intended as a comprehensive change checklist.

Sample Change Analysis Worksheet

Target: _____ Date: _____

FACTORS	EVALUATED SITUATION	COMPARABLE SITUATION	DIFFERENCE	SIGNIFICANCE
WHAT Objects Energy Defects Protective Devices				
WHERE On the object In the process Place				
WHEN In time In the process				
WHO Operator Fellow worker Supervisor Others				
TASK Goal Procedure Quality				
WORKING CONDITIONS Environmental Overtime Schedule Delays				
TRIGGER EVENT MANAGERIAL CONTROLS Control Chain Hazard Analysis Monitoring Risk Review				

To use the worksheet, the user starts at the top of the column and considers the current situation compared to a previous situation and identifies any change in any of the factors. When personnel use this in an accident investigation, they compare the accident situation to a previous baseline. They can evaluate the significance of detected changes intuitively or subject them to the What-If Analysis, Logic Diagram, or other specialized analyses.

CAUSE-CONSEQUENCE ANALYSIS

FORMAL NAME: Cause-Consequence Analysis

ALTERNATIVE NAMES: Cause and Effect Tool, Cause and Effect Diagram, Fishbone Tool, Ishikawa Diagram

PURPOSE: To provide structure and detail as a primary hazard identification procedure. The Cause-Consequence Analysis is a variation of the Logic Tree Tool; personnel use it in the same hazard identification role as the general Logic Diagram. The particular advantage of the Cause-Consequence Analysis is its origin in the quality management process and the thousands of personnel who have been trained in the tool. Because it is widely used, thousands of personnel are familiar with it and, therefore, require little training to apply it to the problem of detecting risk.

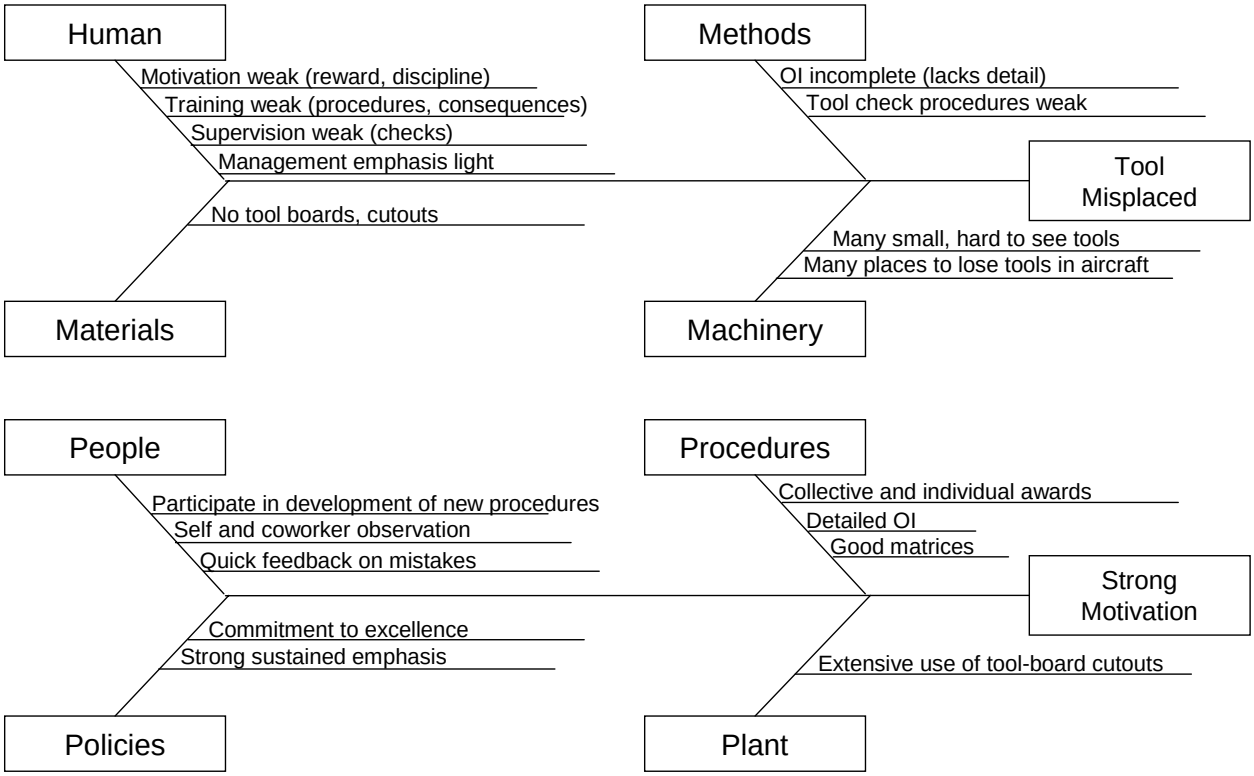
APPLICATION: The Cause-Consequence Analysis is effective in organizations that have had some success with the quality initiative. Personnel should use it in the same manner as the Logic Diagram; they can apply it in both a positive and negative variation.

METHOD: The Cause and Effect Diagram is a Logic Diagram with a significant variation. It provides more structure than the Logic Diagram through the branches that give it one of its alternate names, the Fishbone Tool. The user can tailor the basic “bones” based upon special characteristics of the operation being analyzed. He/she designates either a positive or negative outcome block at the right side of the diagram. Using the structure of the diagram, the user completes the diagram by adding causal factors in either the “M” or “P” structure. Using branches off the basic entries, he/she can add additional hazards. Personnel should use the Cause and Effect Diagram in a team setting whenever possible.

EXAMPLE: The following is an example of the Cause-Consequence Analysis. Using the positive diagram as a guide, the supervisor and working group apply all possible and practical options developed from it (see next page).

SITUATION: The supervisor of an aircraft maintenance operation has been receiving reports from Quality Assurance regarding tools in aircraft after maintenance over the last six months. The supervisor has followed up, but each case has involved a different individual and his spot checks seem to indicate good compliance with tool control procedures. He decides to use a Cause and Effect Diagram to consider all the possible sources of the tool control problem. The supervisor develops the Cause and Effect Diagram with the help of two or three of his best maintenance personnel in a group application.

NOTE: Tool control is one of the areas where 99% performance is not adequate. That would mean that one in a hundred tools is misplaced. The standard is that among the tens (or hundreds) of thousands of individual uses of tools over a year, not one is misplaced.



Using the positive diagram as a guide, the supervisor and working group apply all possible and practical options developed from it.

HAZARD AND OPERABILITY TOOL

FORMAL NAME: Hazard and Operability Tool (HAZOP)

ALTERNATIVE NAMES: HAZOP Analysis

PURPOSE: To analyze hazards of completely new operations. In these situations, traditional, intuitive, and experiential hazard identification procedures are especially weak. This lack of experience hobbles tools such as the What-If Analysis and Scenario Analysis, which rely heavily on experienced operational personnel. The HAZOP deliberately maximizes structure and minimizes the need for experience to increase its usefulness in these situations.

APPLICATION: One should consider the HAZOP when a completely new process or procedure is undertaken. The issue should be one where there is significant risk because the HAZOP demands significant expenditure of effort and may not be cost effective if used against low risk issues. The HAZOP is also useful when an operator or leader senses that “something is wrong” but he/she cannot identify it. The HAZOP will delve deeply into the operation to identify what that “something” is.

METHOD: The HAZOP is the most highly structured of the hazard identification techniques. It uses a standard set of guide terms (below) that are then linked in every possible way with a tailored set of process terms (for example “flow”). Personnel develop the process terms directly from the actual process or from the Operations Analysis. The two words together, for example “no” (a guideword) and “flow” (a process term), will describe a deviation. Personnel then evaluate these deviations to see if a meaningful hazard is indicated. If so, they enter the hazard into the hazard inventory for further evaluation. Because of its rigid process, the HAZOP is especially suitable for one-person hazard identification efforts.

Standard HAZOP Guidewords:

- NO
- MORE
- LESS
- REVERSE
- LATE
- EARLY

Note: This basic set of guidewords should be all that one needs for all applications. Nevertheless, when useful, one can add specialized terms to the list. In less complex applications, only some of the terms may be needed.

INTERFACE ANALYSIS

FORMAL NAME: Interface Analysis

ALTERNATIVE NAMES: Interface Hazard Analysis

PURPOSE: To uncover the hazardous linkages or interfaces among seemingly unrelated activities. For example, if we plan to build a new facility, what hazards may be created for other operations during construction and after the facility is operational? The Interface Analysis reveals these hazards by focusing on energy exchanges. By examining potential energy transfers between two different activities, we can often detect hazards that are difficult to detect by any other means.

APPLICATION: Personnel should construct an Interface Analysis any time they are introducing a new activity and there is any chance at all that unfavorable interaction could occur. A good cue to the need for an Interface Analysis is the use of either the Change Analysis (indicating the injection of something new) or the Map Analysis (with the possibility of interactions).

METHOD: One normally bases the Interface Analysis on an outline such as the one illustrated below. The outline provides a list of potential energy types and guides the consideration of the potential interactions. One makes a determination as to whether a particular type of energy is present and then whether there is potential for that form of energy to adversely affect other activities. As in all aspects of hazard identification, the creation of a good Operations Analysis is vital.

The Interface Analysis Worksheet

Energy Element:
- Kinetic (objects in motion)
- Electromagnetic (microwave, radio, laser)
- Radiation (radioactive, x-ray)
- Chemical
- Other

Personnel Element: Personnel moving from one area to another
Equipment Element: Machines and material moving from one area to another
Supply/Materiel Element:
- Intentional movement from one area to another
- Unintentional movement from one area to another

Product Element: Movement of product from one area to another
Information Element: Flow of information from one area to another or interference (i.e., jamming)
Bio-material Element:
- Infectious materials (virus, bacteria, etc.)
- Wildlife
- Odors

ACCIDENT/INCIDENT ANALYSIS

FORMAL NAME: Accident/Incident Analysis

ALTERNATIVE NAMES: Accident Analysis

PURPOSE: Most organizations have accumulated extensive, detailed databases that are gold mines of risk data. The purpose of the analysis is to apply this data to the prevention of future accidents or incidents.

APPLICATION: Every organization should complete an operation incident analysis annually. The objective is to update the understanding of current trends and causal factors. The organization should complete the analysis for each organizational component that is likely to have unique factors.

METHOD: One can approach the analysis in many ways. The process generally builds a database of the factors listed below, which serves as the basis to identify the risk drivers. Typical factors to examine include the following:

- Activity at the time of the accident
- Distribution of incidents among personnel
- Accident locations
- Distribution of incidents by sub-unit
- Patterns of unsafe acts or conditions

JOB SAFETY ANALYSIS

FORMAL NAME: Job Safety Analysis (JSA)

ALTERNATIVE NAMES: Job Hazard Analysis (JHA), Task Hazard Analysis (THA)

PURPOSE: Examine, in detail, the safety considerations of a single job. A variation of the JSA, called a Task Hazard Analysis, focuses on a single task (i.e., some smaller segment of a "job").

APPLICATION: Some organizations have established the goal of completing a JSA on every job in the organization. If this can be accomplished cost effectively, it is worthwhile. Certainly, the higher risk jobs in an organization warrant application of the JSA procedure. Within the risk management approach, it is important that an organization accomplish such a plan by beginning with the most significant risk areas first.

The JSA is best accomplished using an outline similar to the one illustrated below. As shown in the illustration, the organization breaks down the job into its individual steps. The organization should handle jobs that involve many very different tasks by analyzing each major task separately. The illustration considers risks both to the workers involved and to the system, as well as risk controls for both. Tools such as the Scenario and What-If Analysis can contribute to the identification of potential hazards. There are two alternate ways to accomplish the JSA process. A safety professional can complete the process by asking questions of the workers and supervisors involved. Alternatively, supervisors can be trained in the JSA process and be directed to analyze the jobs that they supervise.

Sample Job Hazard Analysis Format from OSHA 3071 2002 (Revised):

Job Title:	Job Location:	Analyst	Date
Task #	Task Description:		
Hazard Type:	Hazard Description:		
Consequence:	Hazard Controls:		
Rationale or Comment:			

ENERGY TRACE AND BARRIER ANALYSIS

FORMAL NAME: Energy Trace and Barrier Analysis (ETBA)

ALTERNATIVE NAMES: Energy Trace-Barrier Analysis, Abnormal Energy Exchange

PURPOSE: To detect hazards by focusing in detail on the presence of energy in a system and the barriers for controlling that energy. It is conceptually similar to the Interface Analysis in its focus on energy forms, but is considerably more thorough and systematic.

APPLICATION: The ETBA is intended for use by system safety professionals and is targeted against higher risk operations, especially those involving large amounts of energy or a wide variety of energy types. Personnel use the method extensively in the acquisition of new systems and other complex systems.

METHOD: The ETBA consists of the following five basic steps:

- Step 1. Identify the types of energy present in the system
- Step 2. Locate energy origin and trace the flow
- Step 3. Identify and evaluate barriers (mechanisms to confine the energy)
- Step 4. Determine the risk (the potential for hazardous energy to escape control and potentially create a hazard)
- Step 5. Develop improved controls and implement as appropriate

Types of Energy:

- Electrical
- Kinetic (moving mass, e.g., a vehicle, a machine part, a bullet)
- Potential (non-moving mass, e.g., a heavy object suspended overhead)
- Chemical (e.g., explosives, corrosive materials)
- Noise and vibration
- Thermal (heat)
- Radiation (non-ionizing, e.g., microwave and ionizing, e.g., nuclear radiation, x-rays)
- Pressure (air, hydraulic, water)

FAULT TREE ANALYSIS

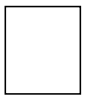
FORMAL NAME: Fault Tree Analysis (FTA)

ALTERNATIVE NAMES: Logic Tree

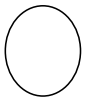
PURPOSE: To add hazard identification value to the basic Logic Diagram. The Fault Tree Analysis (FTA) is a hazard identification tool based on the negative type Logic Diagram. The FTA adds several dimensions to the basic logic tree. The most important of these additions is the use of symbols to add information to the trees and the possibility of adding quantitative risk data to the diagrams.

APPLICATION: Because of its relative complexity and detail, it is normally not cost effective to use the FTA against risks assessed below the level of extremely high or high. Personnel use the method extensively in the acquisition of new systems and other complex systems where, due to the complexity and criticality of the system, the tool is a must.

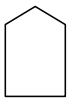
METHOD: One constructs the FTA using the following symbols:



The output event. Identification of a particular event in the sequence of an operation.

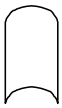


A basic event. An event, usually a malfunction, for which further causes are not normally sought.

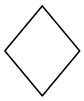


A normal event. An event in an operational sequence that is within expected performance standards

An "AND" gate. Requires all of the below connected events to occur before the above connected event can occur



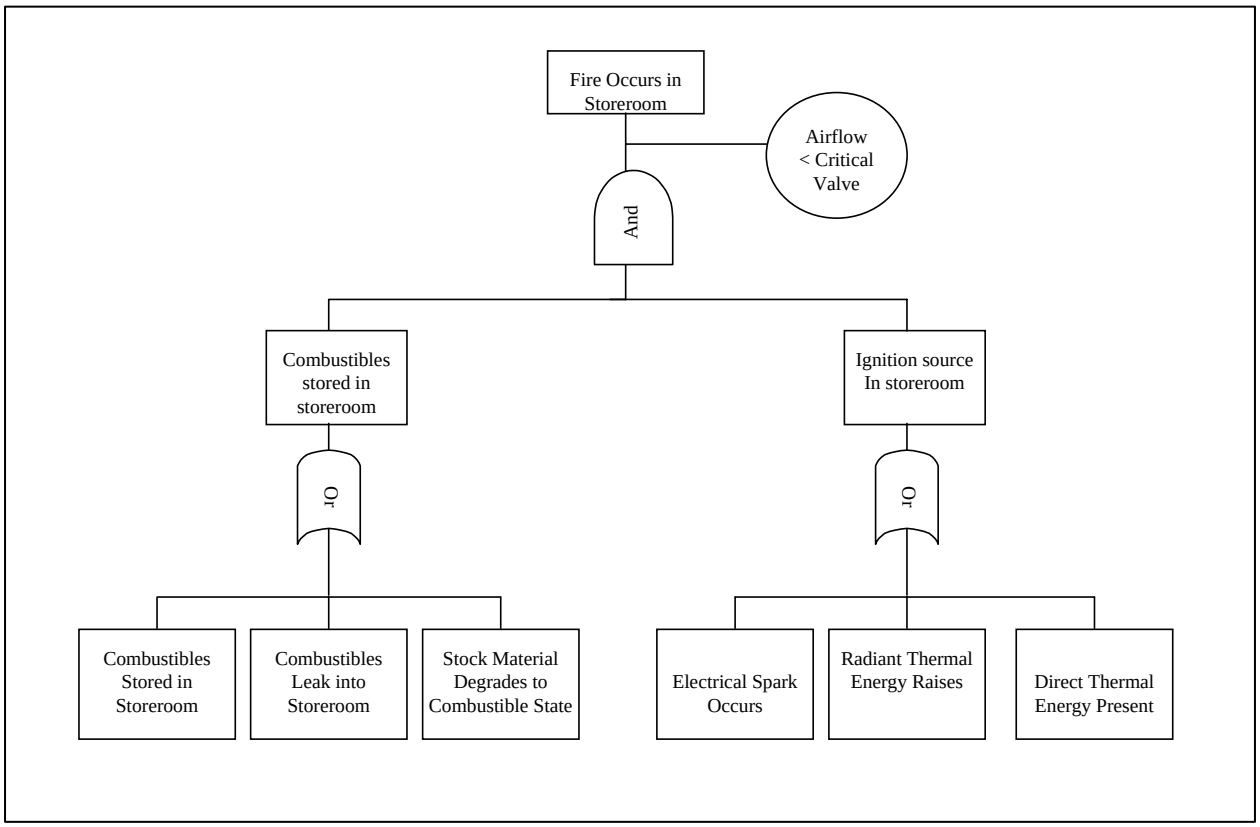
An "OR" gate. Any one of the events can independently cause the event placed above the OR gate



An undeveloped event. This is an event not developed because of lack of information or the event lacks significance.

Transfer symbols. These symbols transfer the user to another part of the diagram. These symbols are used to eliminate the need to repeat identical analyses that have been completed in connection with another part of the fault tree.

EXAMPLE: A brief example of the FTA illustrates how one can trace an event to specific causes that he/she can very precisely identify at the lowest levels. See below for an example of the FTA.



MANAGEMENT OVERSIGHT AND RISK TREE

FORMAL NAME: Management Oversight and Risk Tree (MORT)

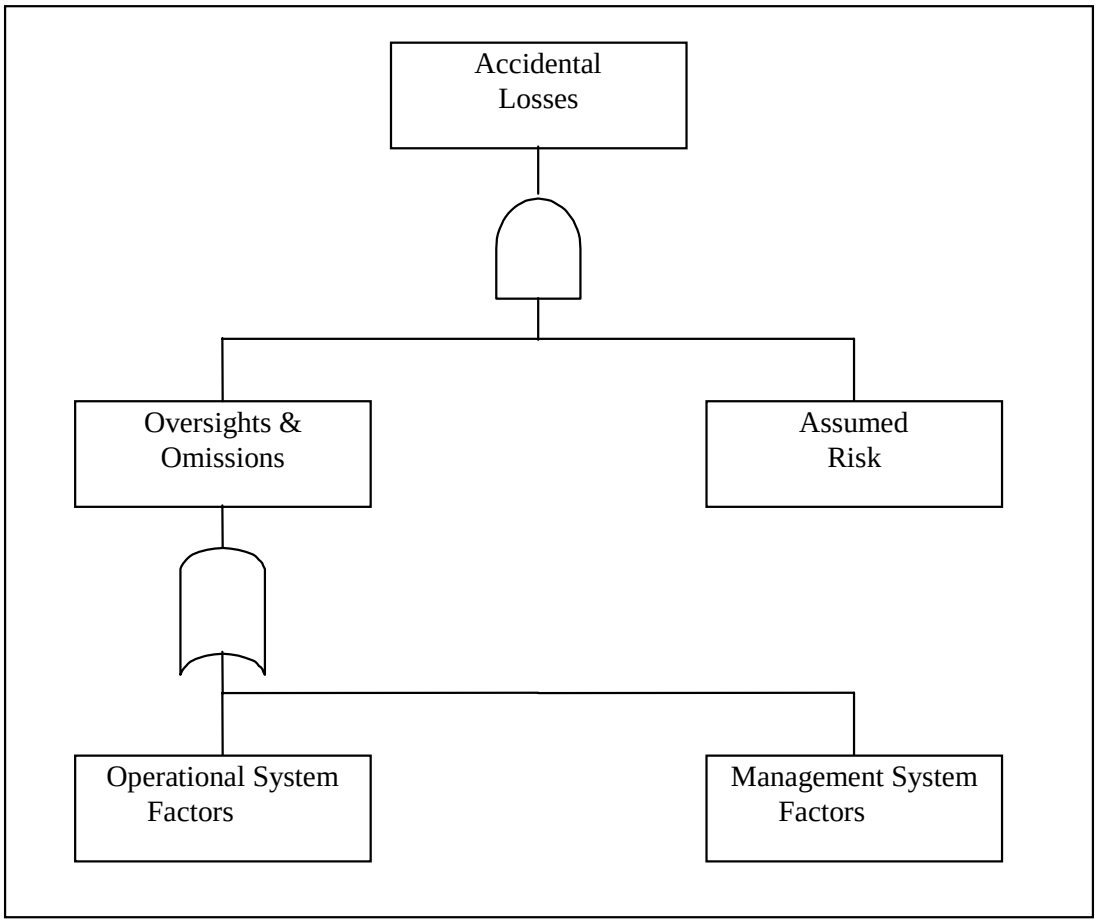
ALTERNATIVE NAMES: None

PURPOSE: To identify hazards. The Management Oversight and Risk Tree (MORT) uses a series of charts developed and perfected over several years by the Department of Energy in connection with their nuclear safety programs. Each chart identifies a potential operating or management level hazard. The attention to detail characteristic of MORT is illustrated by the fact that the full MORT diagram or tree contains more than 10,000 blocks. Even the simplest MORT chart contains over 300 blocks. The full application of MORT is a time-consuming and costly venture. One can routinely use the basic MORT chart with about 300 blocks as a check on other hazard identification tools. By reviewing the major headings of the MORT chart, an analyst will often be reminded of a type of hazard that was overlooked in the initial analysis. The MORT diagram is also very effective in ensuring attention to the underlying management root causes of hazards.

APPLICATION: Full application of MORT is reserved for the highest risks and most operation-critical activities because of the time and expense required. MORT generally requires a specially trained loss control professional to assure proper application.

METHOD: MORT is accomplished using the MORT diagrams, of which there are several levels available—the most comprehensive, with about 10,000 blocks. There is an intermediate diagram of approximately 1500 blocks and a basic diagram with about 300. It is possible to tailor a MORT diagram by choosing various branches of the tree and using only those segments. The MORT is essentially a negative tree, so the process begins by placing an undesired loss event at the top of the diagram used. The user then systematically responds to the issues posed by the diagram. All aspects of the diagram are considered and the “less than adequate” blocks are highlighted for risk control action.

EXAMPLE: The diagram illustrated on the next page is a section of a MORT diagram.


Accidental Losses
Oversights & Omissions
Assumed Risk
Operational System Factors
Management System Factors

HUMAN ERROR ANALYSIS

FORMAL NAME: Human Error Analysis (HEA)

ALTERNATIVE NAMES: Human Error Management; Human Reliability Analysis, Threat and Error Management

PURPOSE: To identify, analyze, and mitigate safety hazards associated with human error.

APPLICATION: In the domain of safety, human performance degradation and error have a constant, diffuse presence. There is, in fact, no such thing as error-free human performance over any meaningful time period. Errors happen to people. Accordingly, there is a need to identify hazards related to human error during the development of complex systems and the allied procedures. This entails the prospective and retrospective analysis of human error and how it is used to manage safety risk as part of the system design process.

METHOD: One assesses and either mitigates or accepts the risk for each hazard as a part of the ATO SMS. There is a multitude of safety analysis tools that human factors practitioners can apply to identify and resolve risks associated with human-system reliability. The foundation of such analyses is a Task Analysis that describes and details human-to-system interactions. The complexity and detail practitioners include is dependent upon the complexity of the system and the issue under study. Typically, more complex analyses include the preparation of Operation Sequence Diagrams (OSDs) that detail the sequence and timing of human-to-system and system-to-human interactions. For a relatively simple problem, a Functional Task Flow expanded for “wrong” decisions may be adequate. For complex systems, more powerful and comprehensive analysis tools may be required. Practitioners use these to evaluate each human decision point for system impact if an error is made. From these analyses, they can develop mitigations and controls.

The products of the tools should be geared toward aiding FAA management in risk management in the area of the human element of system, procedure, facility, and workplace environment design. These tools enable human factors practitioners to identify human error hazards during all stages of the change process at the appropriate level of detail such that human factors professionals can communicate the gravity of the risk and how to effectively control the hazard. Human Factors practitioners make the results of the analysis usable by system engineering personnel, program managers, procedure designers, and other decision-makers so that they can select alternatives to achieve a risk-based cost-effective result.

EXAMPLE: To implement a proactive method for analyzing the risk of human error and safety associated with systems and procedures used in air traffic control facility maintenance, the FAA modified an approach called Human Error and Safety Risk Analysis (HESRA). HESRA is a method that has been shown to be workable, applicable, and effective in identifying and mitigating the conditions that are likely to increase human errors in maintenance processes. HESRA accepts the error research and classification schemes that identify human error as skill-based, rule-based, and knowledge-based errors, and those categorized as slips, mistakes, violations, errors of commission, and errors of omission. Since most errors have little or no consequence, HESRA recognizes that bad events that occur as the result of human errors are usually the product of a “chain of causation,” (i.e., a link in a causative chain of events that can have dramatic consequences). The HESRA approach capitalizes on “chain of causation” characteristics of major accidents to: 1) identify and eliminate conditions that elevate the risk of

errors, and 2) provide “cutouts” that short circuit the chain of causation, so isolated errors are not allowed to propagate to an ultimate (bad) event. Since it is an *a priori* method, practitioners can apply HESRA at virtually any stage of the system design, procurement, and implementation cycle. HESRA is based on a well-developed and widely practiced engineering risk assessment technique known as Failure Mode and Effect Analysis, or FMEA. There are a number of existing commercial software applications that support FMEA activities and data. Practitioners can adapt several of these tools to support HESRA. The pre-requisite for conducting a HESRA analysis is that practitioners must define the interaction process among human users and the system in enough detail to permit its decomposition into tasks and steps.

JOB TASK ANALYSES

FORMAL NAME: Job Task Analyses (JTA)

ALTERNATIVE NAMES: Task Analysis; Cognitive Task Analysis (CTA)

PURPOSE: To identify and analyze human tasks within a system, including human-to-system interaction points. A task analysis describes each human task/sub-task within a system in terms of the perceptual (information in-take), cognitive (information processing and decision making), and manual (motor) behavior required of an operator, maintainer, or support person. It should also identify the skills and information required to complete the tasks; equipment requirements; the task setting (environment); time and accuracy requirements; and the probable human errors and consequences of these errors. There are several tools and techniques for performing task analyses, depending upon the level of analysis needed.

APPLICATION: Personnel use task analyses to define, evaluate, and document human functions and task flows throughout systems development and/or modification. Task analyses provide visual, graphic representations that permit users to analyze human-to-system interactions for efficiency and impact of human error.

For each task, the minimum data one collects and analyzes should be:

- Equipment acted upon
- Consequence of the action
- Feedback information resulting from the action
- Criterion of task accomplishment
- Estimate of probability of error
- Estimate of time to perform the task successfully
- Relation of the time and error rate associated with each critical task to the performance time and error rate for the overall system

METHOD: There are many tools available to support job task analyses. One selects them for a particular application depending upon the purpose of the analysis, the amount of detail required, and the point during systems design and/or analysis to which they are being applied. Methods that one may use include: Functional Flow Diagrams, Flow Process Charts (FPC), Decision/Action Diagrams, and Operational Sequence Diagrams (OSDs).

Functional Flow Diagrams - Also referred to as functional block diagrams, functional flows, and functional flow block diagrams these diagrams graphically depict system functions and the sequence and interrelationships of these functions. Initial diagrams are high level and do not include function allocation. As the analysis progresses, levels of detail are added such as function allocation, data/information interchange, frequency, and timing. Arrows indicate the normal sequence of functions. Reference block numbering indicates the function level and association for traceability as functions are decomposed. Points at which arrows join or split are connected by "and," "or," or "and/or" junctions or gates. Users decompose functional flow diagrams into multiple levels of finer detail. Users can expand functional flow diagrams for simple systems for “wrong” decisions and use them to address human error.

Flow Process Charts - Personnel use these charts to depict the sequence of user activities or information transfer as part of a system. An FPC is vertically oriented and can be annotated on

either side with a time scale if the data is available. Personnel develop these charts to detail operator tasks and incorporate human and machine/system decision points.

Decision/Action Diagrams - These diagrams are similar to functional flows except that users add decision points. They express each function as a "verb-noun" combination with occasional adjectives or other modifiers. They place each decision point in a diamond-shaped outline symbol and write it in question form. The question must be binary, answerable by a "yes" or "no" response. Users label both functional action blocks and decision diamonds with reference numbers, similar to those used for functional flow diagrams. Reference numbers are necessary to ensure traceability. Personnel can use these diagrams to support a Human Error Analysis (HEA).

Operational Sequence Diagrams - OSDs are similar in format to Flow Process Charts (FPCs) in that they depict "top-down" sequential user and equipment task flows. However, OSDs contain much more information and are particularly suited to the analysis of complex systems with many time critical information-decision-action interactions between several users and equipment items. OSDs indicate actions; decisions; inspections; data transmitted, received, or stored; and the timing of these events. While OSDs are more difficult to develop, they are very powerful analysis tools, enabling clear visualization of the user and equipment interrelationships, human-machine interfaces, information interchange, task flow, task frequency, and workload. Because of their completeness in documenting operator and equipment interactions, OSDs frequently form the basis of HEA and personnel use them to evaluate each human decision point for system impact if an error is made. From these analyses, personnel can develop mitigations and control.

Appendix H – Documenting Existing Hazards Process

This appendix explains the existing hazard documentation process. During Phase 2 of the SRM process, the SRM Panel identifies hazards for the NAS change undergoing the analysis. Those hazards fall into three categories:

1. Pre-existing hazards *not in scope* and *not caused* by the change
2. Pre-existing hazards *in scope* and *not caused by* the change
3. Hazards *in scope* and *caused by* the change

The scope refers to whether or not the hazard falls within the system description determined in Phase 1 of the SRM process. In describing the system, the SRM Panel bounds the system; which means limiting the analysis of the change or system to the elements that affect or interact with each other to accomplish the central function. An identified hazard may or may not be within the newly bounded system and therefore, determines whether it is in or out of the scope of the change.

Each of the three categories of hazards listed above follow a specific process for ensuring ownership, documentation, and monitoring. The following diagram provides an overview of the processes to follow for each hazard type.

As shown in Figure H.1, Documenting Existing Hazards Process Flow Chart, the SRM Panel first identifies a hazard. The SRM Panel then decides which of the three categories the hazard falls into:

1. Pre-existing hazards *not in scope* and *not caused by* the change
2. Pre-existing hazards *in scope* and *not caused* by the change
3. Hazards *in scope* and *caused by* the change

If the hazard is pre-existing, not within the scope of the change (i.e., not within the bounded system as described earlier), and not directly caused by the change, the SRM Panel facilitator follows “Path A” in the diagram. If the hazard is pre-existing, within the scope of the change, but not directly caused by the change, the SRM Panel facilitator follows “Path B” in the diagram. If the hazard is both within the scope of the change and directly caused by the change, the SRM Panel follows “Path C” in the diagram. Below are details on the specific steps within each path.

Path A

A1. The SRM Panel identifies that the hazard is pre-existing, not in scope, and not caused by the change. Go to step A2.

A2. The SRM Panel documents the hazard and ownership in the SRMD for the current change. The risk level of this hazard is not assessed by the SRM Panel, it is only identified; therefore, the risk associated with the identified existing hazard is not included in the risk acceptance of the SRMD. Go to step A3.

A3. The SRM Panel identifies the appropriate Service Unit owner. If unsure of the owner, the facilitator works with his/her Safety Engineer to determine appropriate ownership. Once determined, the facilitator informs his/her Service Unit Safety Office, as well as the ATO SRM Office. Go to step A4.

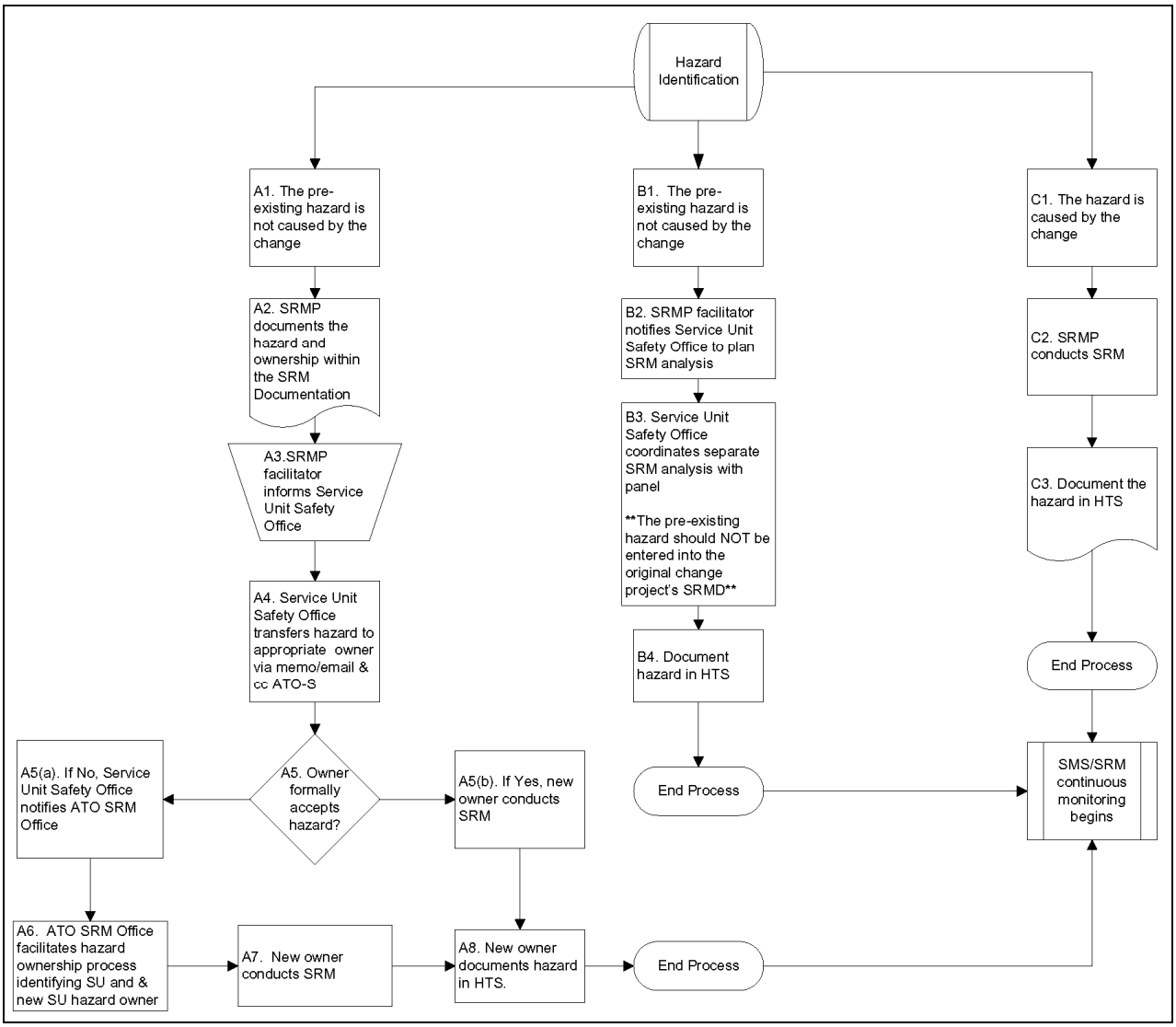


Figure H.1: Documenting Existing Hazards Process Flow Chart

A4. The identifying Service Unit Safety Office transfers the hazard to the appropriate owner by sending a memo documenting the hazard and the intended transfer of ownership. To expedite the process, the identifying Safety Office sends the memo in hard copy as well as e-mails it to the appropriate party, copying the ATO SRM Office on all correspondence. It is recommended that this correspondence be included in the SRMD. Go to step A5.

A5. The identifying Service Unit Safety Office determines that the new owner formally accepts the hazard by receipt of a formal acceptance memo. If no, go to step A5(a). If yes, go to step A5(b).

A5(a). If the identifying Service Unit Safety Office is not in receipt of a memorandum from the new owner formally accepting the hazard; notify the ATO SRM Office. Go to step A6.

A6. The ATO SRM Office works with the Safety Offices of the identifying Service Unit and the suggested new Service Unit owner to facilitate hazard ownership. Go to step A7.

A7. The new owner follows the SRM process to assess the hazard and determine the next steps. The ATO SRM Office reviews the SRMD or SRMDM. Go to step A8.

A5(b). The identifying Service Unit Safety Office determines that the owner has formally accepted the hazard by receipt of a formal acceptance memo. The new owner follows the SRM process to assess the hazard and determine next steps. The ATO SRM Office reviews the SRMD or SRMDM. Go to step A8.

A8. The new owner documents the hazard in the hazard tracking system. The documenting existing hazards process ends for this hazard and continuous monitoring begins.

Path B

B1. The SRM Panel identifies that the hazard is pre-existing, in scope, and not caused by the change. Go to step B2.

B2. The SRM Panel facilitator notifies his/her Service Unit Safety Office to plan a future SRM Panel to assess the identified hazard. Go to step B3.

B3. The Service Unit Safety Office coordinates a separate SRM analysis (separate from the original change project) with an SRM Panel. Go to step B4.

B4. The SRM Panel facilitator works with the appropriate party to document the hazard in the hazard tracking system. The documenting existing hazards process ends for this hazard and continuous monitoring begins.

Path C

C1. The SRM Panel identifies that the hazard is in scope and caused by the change. Go to step C2.

C2. The SRM Panel conducts the SRM analysis on the NAS change, including the hazard in the process. Go to step C3.

C3. The SRM Panel facilitator works with the appropriate party to document the hazard in the hazard tracking system. The documenting existing hazards process ends for this hazard and continuous monitoring begins

Appendix I – Bow-Tie Model Example

This appendix provides an example of the use of the Bow-Tie Model using a hazard related to (the implementation of) Reduced Vertical Separation Minimum (RVSM) in the West Atlantic Route Structure (WATRS) region.

RVSM Background

The feasibility of reducing Vertical Separation Minimum (VSM) above Flight Level (FL) 290, while maintaining an equivalent level of safety, is dependent on operational judgment and a thorough assessment of associated risks. The total risk associated with RVSM is a derivative of two factors: the technical risk due to aircraft height-keeping performance and the operational risk due to any vertical deviation of aircraft from their cleared flight levels due to error by the flight crew or Air Traffic Control (ATC). The overall collision risk within RVSM airspace is assessed against a Target Level of Safety (TLS) of $5x10^{-9}$ fatal accidents per flying hour.

RVSM reduces the vertical separation for FL290 through FL410 from the traditional 2,000-foot minimum to 1,000-foot separation. RVSM creates exclusionary airspace and only approved aircraft may operate within the stratum. This airspace change adds six additional flight levels, which create benefits for Air Traffic Service (ATS) providers and aircraft operators. The additional flight levels enable aircraft to safely fly more optimal profiles, gain fuel savings, and increase airspace capacity. The process of changing this separation standard requires a safety analysis to determine the actual performance of airspace users under the current separation minimum (2,000 feet) and potential performance under the new standard (1,000 feet). In 1988, the International Civil Aviation Organization (ICAO) Review of General Concept of Separation Panel (RGCSP) completed this study and concluded that safe implementation of the 1,000-foot separation standard was technically feasible. Figure I.1 illustrates conventional separation versus RVSM.

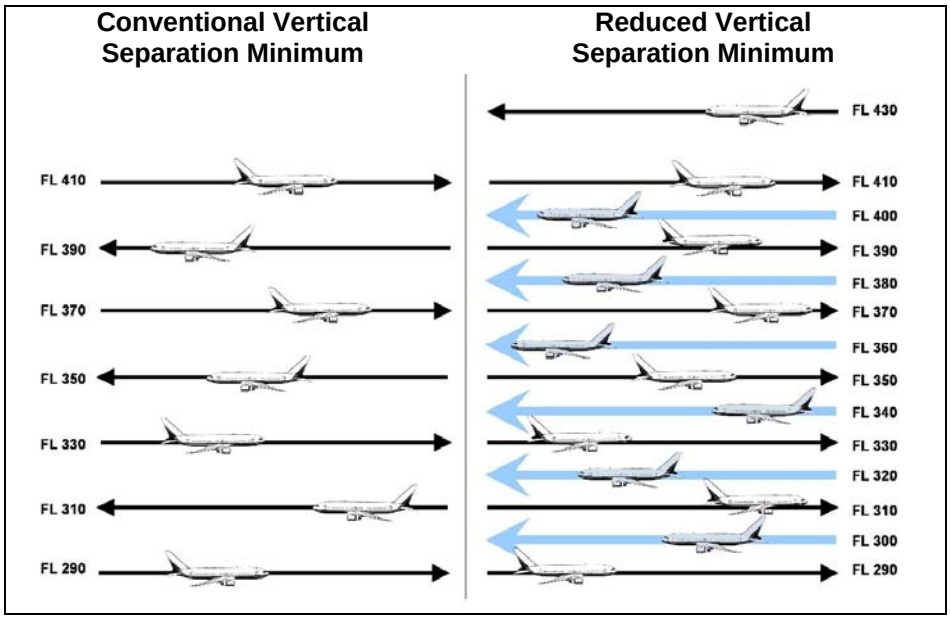


Figure I.1: Conventional 2,000-Foot Separation Minimum vs. RVSM

(Note: RVSM creates six additional flight levels for airspace users and ATS providers to utilize.)

While RVSM airspace (FL290 through FL410) is exclusive for those aircraft certified and approved for operation in that environment, the Federal Aviation Regulations (FARs) also allow for limited accommodation of certain exception groups. The exceptions include:

- Department of Defense (DoD) aircraft
- Humanitarian or Lifeguard aircraft
- Foreign State aircraft
- Manufacturer aircraft being flown for certification/development

ATS providers will only accommodate these exception group aircraft when workload permits them to do so. The DoD need for accommodation is primarily for strategic aircraft such as fighters and bombers due to the inability to install upgrade packages in those aircraft. The other exception group categories cover a broader range of aircraft and are also accommodated on a "workload permitting" basis. Operators requiring routine access into RVSM airspace are advised to upgrade their aircraft as non-approved aircraft create a significant controller workload due to the fact that different separation standards must be applied for those aircraft. Non-approved aircraft are easily identified by the absence of the equipment suffix "/W" in the filed aircraft flight plan. All conflict probe and conflict alert functions have been modified to recognize the difference between such aircraft to aid the controller and ensure system integrity. An indicator for any aircraft that is not approved for RVSM is provided by a visual cue for the controller when such an aircraft is present on the radar display. Extensive coordination procedures have been designed to ensure that workload is properly controlled and managed.

Numerous Regions have safely implemented RVSM since the initial North Atlantic (NAT) implementation in March 1997. The FAA provides a safety oversight function of the maintenance of the TLS for the two RVSM Regions currently under their control: the Pacific (PAC) and the West Atlantic Route System (WATRS).

Implementing RVSM in the WATRS Region

Although RVSM has already been implemented in the WATRS Region (see Figure I.2), this example was developed under the assumption that the WATRS Region was only being considered for RVSM implementation.

Despite the fact that both operational risks and technical risks are assessed prior to RVSM implementation, this example will focus on factors contributing to operational risk. The system was bounded to exclude factors contributing to technical risk and assumes that the Altimetry System Error (ASE) of all participating approved aircraft is zero feet. This assumption does not include large height deviations due to other technical risk factors.

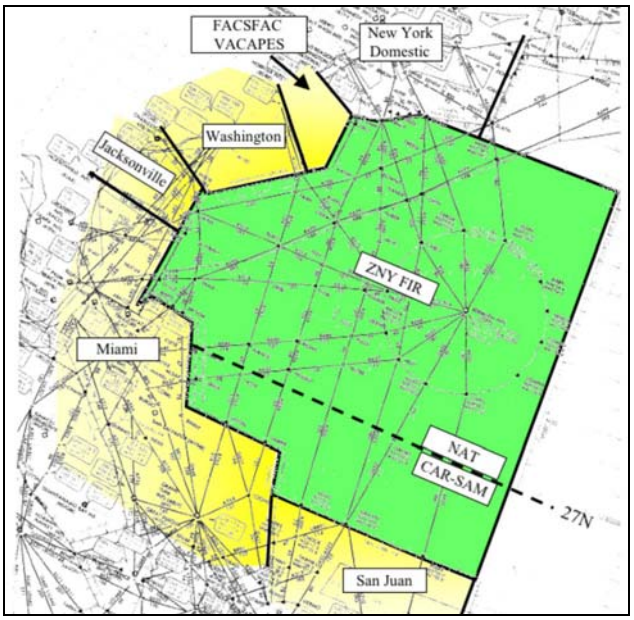


Figure I.2: WATRS RVSM

(Note: The airspace is depicted by the green polygon.)

WATRS RVSM was presumably implemented in November 2001. This exclusionary airspace is under control of New York ARTCC (ZNY) and borders Washington, Jacksonville, and Miami Air Route Traffic Control Centers (ARTCCs), along with the San Juan Combined Center Radar Approach Control (CERAP). The number of WATRS RVSM operations averages approximately 2,000 flights per week.

Successful airspace modifications, such as RVSM implementation, are dependent on full understanding and execution of each of the pieces required for implementation. The FAA will work from a general or tailored checklist in which items may include (but are not limited to):

- Rulemaking (Proposed and Final Rulemaking Packages)
- Guidance material development
- Operator requirements (Minimum Equipment List (MEL)) to conduct operations within RVSM altitudes FL290 through FL410
- ATC coordination
  - Internal to the facility
  - External to the facility
  - Users/operators
- ATC Automation Requirements
- ATC and operator flight crew training
- Document modifications
- Other publications
- Operator aircraft readiness target for go/delay decision
- Aircraft monitoring requirements

As with any change in the NAS, RVSM requires careful consideration, as well as a description and analysis of all of the system elements involved. Depending on the purpose or the magnitude of the modification, the relative importance of each of the elements may vary.

Large Height Deviation Hazard Bow-Tie

One of the hazards identified for (the implementation of) RVSM is a Large Height Deviation (LHD). Any deviation from the assigned or anticipated altitude (that altitude that the controller believes the aircraft to be at, or the pilot believes he/she is to be at, or that the aircraft is climbing or descending to) of 300 feet or greater constitutes a large height deviation.

Figures I.3, I.4, and I.5 illustrate the analysis of the LHD hazard using the Bow-Tie model. Figure I.3 provides a simplified overview of the LHD hazard, with some of the high-level causes identified on the left side in rectangles. These causes can then be broken down further into sub-causes. To the right of the hazard, the system states associated with the hazard are identified. In essence, Figure I.3 summarizes the two main identified potential outcomes, namely 'Mid-Air Collision' and 'Loss of Separation.' The effects have then been rated for severity in accordance with Table 3.3, indicating four catastrophic potential outcomes and four minor potential outcomes.

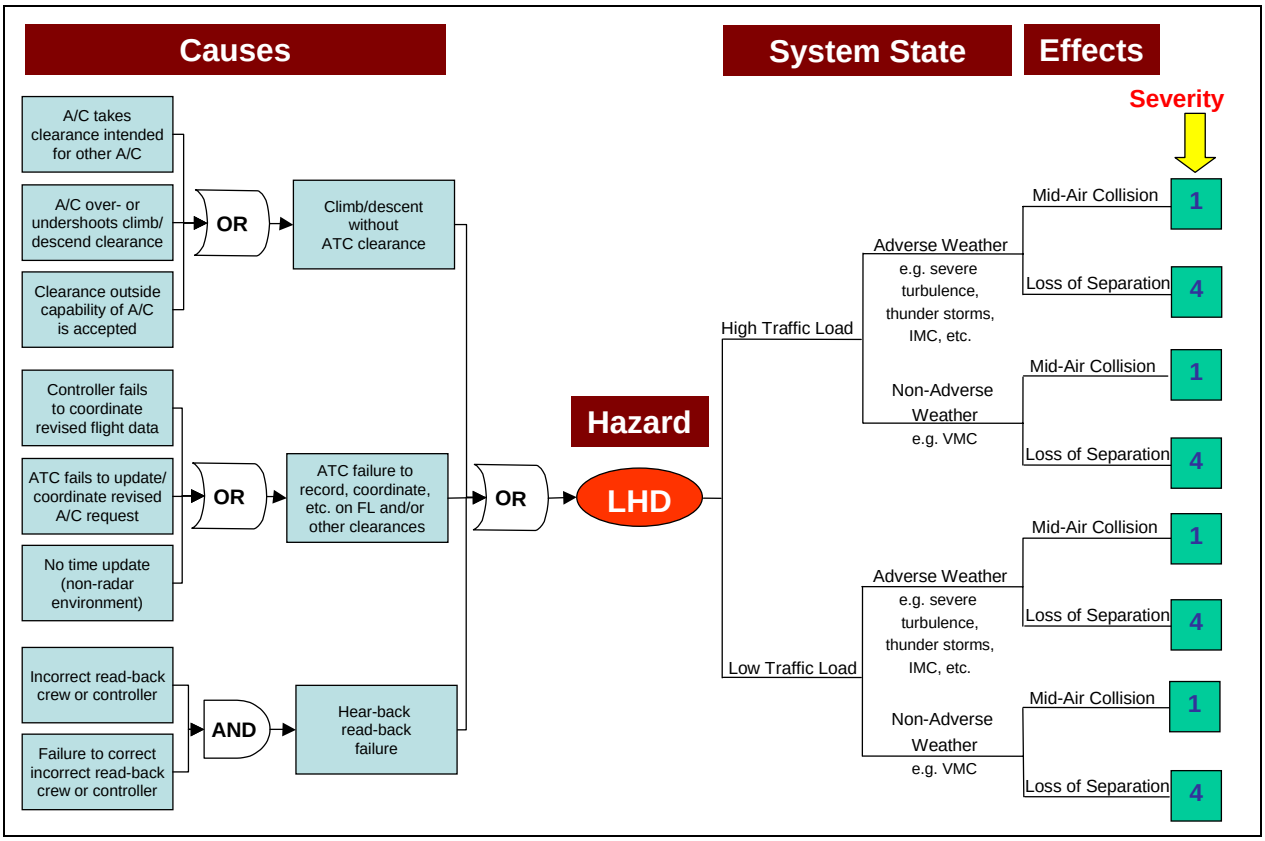


Figure I.3: Bow-Tie Model: Large Height Deviation - Severity

Data collected in order to calculate the different likelihood values consisted of:

- WATRS Airspace statistics, including the distribution of monthly traffic volume within the WATRS RVSM stratum
- Height Deviation Reports for 2004
- Forecasted convective weather days for 2004
- A note on the Height Deviation Reports for 2004 in the data package states: "It was determined that in three instances of height deviations, there was loss of separation."

- The probability of a Mid-Air Collision in the WATRS Region was extracted from the Safety Risk Management: Worst Credible Outcome Likelihood Values for Mid-air Collisions (MACs) and Controlled Flights into Terrain (CFITs), August 24, 2005, by using the MAC Probability Value in an En Route environment.

The likelihood of the potential outcomes can then be calculated based on the information gathered, for which the results are shown in Figures I.4 and I.5. The values can consequently be rated in accordance with Table 3.4.

Note: The validity and completeness of (available) data or representative SMEs play a major role in the validity of the calculated likelihoods for the different scenarios.

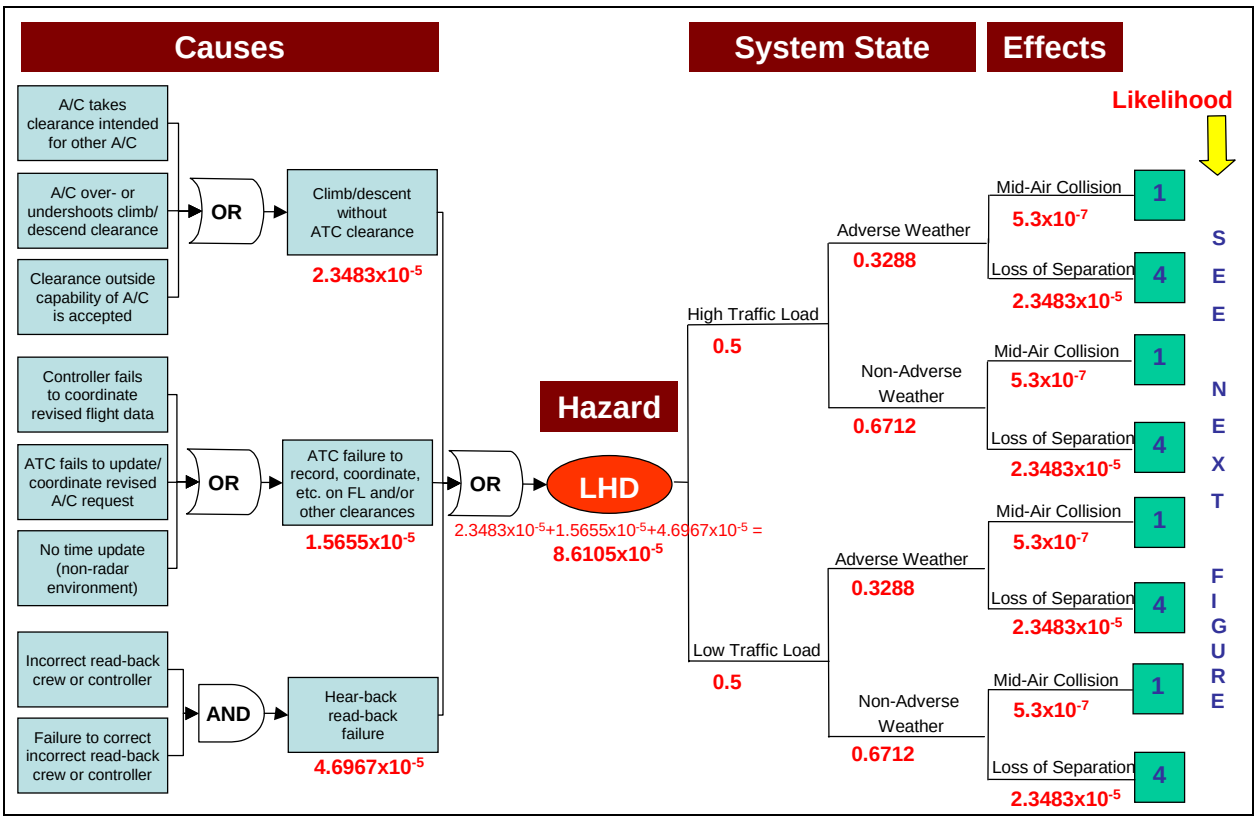


Figure I.4: Bow-Tie Model: Large Height Deviation - Likelihood

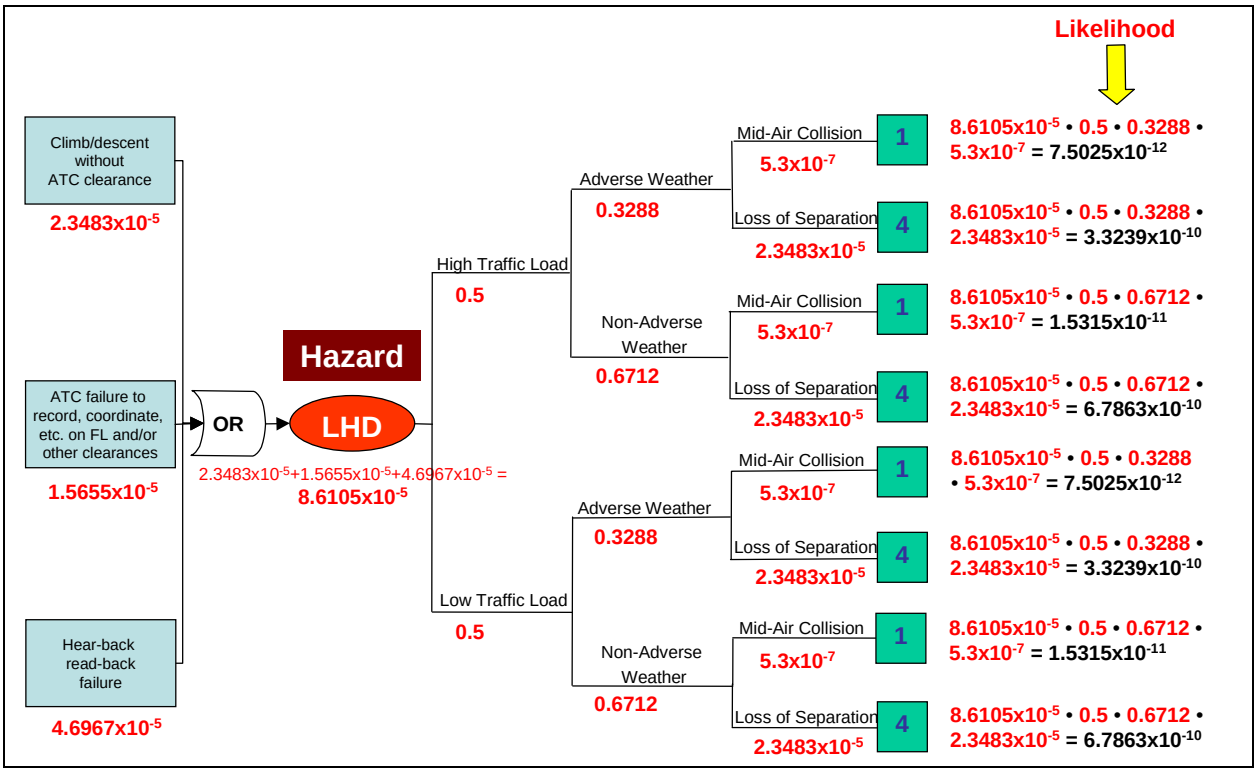


Figure I.5: Bow-Tie Model: Large Height Deviation – Likelihood (continued)

Appendix J – High-level SRMD Guidance

NOTE 1: This outline provides some general instructions based on the requirements discussed in Section 3.12 of the ATO SMS Manual, Version 2.1. This is guidance; the SRMD should be tailored to the proposed change.

NOTE 2: New system acquisitions that are subject to the FAA AMS should use the SRMGSA document for guidance in preparing the SRMD.

SRMD Change Page
Include a table listing changes made to the different versions of the SRMD, including the corresponding date and version number.

Signature Page
The signature page should contain the following information:

Title: A clear and concise description of the proposed change
Originator Information: Originator's name, organization, contact information, etc.
SRMD Information: SRMD submission date, SRMD revision number, etc.
Reviewer Information: If the SRMD has gone through a peer-review prior to being submitted for approval, concurrence should be noted. Includes reviewer signature(s), name(s), organization(s), and date.
SRMD Approval and Risk Acceptance Signature(s): The necessary signatures required for SRMD Approval and Risk Acceptance. Chapter 3, *Safety Risk Management*, Section 3.12 of the *ATO SMS Manual, Version 2.1*, provide guidance regarding who should approve the SRMD. Chapter 3, Sections 3.14.2 – 3.14.3 of the *ATO SMS Manual, Version 2.1,* provides guidance regarding risk acceptance requirements.
Proposal Rejection: When a proposed change is considered unsafe for implementation, such a decision should be recorded in the SRMD, with accompanying rationale, and appropriate signatures.

Executive Summary
The summary should give a general description of the proposed change/procedure, including a list of the hazards with associated high or medium risks and their corresponding initial and predicted residual risk. Include a high level system description, a summary of how the SRMD was developed, and what process/method was used to move through the SRM process.

Introduction
Provide a brief reasoning/rationale for the change/procedure initiative. The scope of the change, whether it is more complex or far-reaching, will determine the need for increased scope and detail of the analysis to be performed.

Section 1 – Current System/System Baseline
In this section, provide a description of the current system or existing procedures, as well as corresponding (operational) system states. If the proposal entails a procedural change, describe the current procedure and its operational environment. If the current system or procedure is unique and has challenges associated with its unique situation, be sure to point these out.

Section 2 – Proposed Change
This section should give a description of the proposed change/procedure, identifying which safety parameters are involved.

Section 3 – Safety Risk Management Planning and Impacted Organizations
Prior to initiation of the safety analysis, SRM planning is necessary. It is essential to select the appropriate SRM participants, identify the SRM Panel, schedule milestones, and assign tasks and responsibilities. With regards to the organizations that are impacted by the change, describe the method used for collaboration between those organizations during the identification, mitigation, tracking, and monitoring of hazards associated with the change. The information provided in this section should meet the requirements outlined Sections 3.4.1 - 3.4.3 of the *ATO SMS Manual, Version 2.1*.

Section 4 – Assumptions
If in the process of modifying an existing system or developing a procedure any assumptions are made in order to make the evaluation of the change more manageable, clearly define and document them in this section.

Section 5 – Phase 1: System Description
The system description should provide a description of the system/procedure, its operational environment, the people involved/affected by the change/procedure, and the equipment required to accommodate the change, while meeting the requirements outlined in Section 3.7 of the *ATO SMS Manual, Version 2.1*.

Section 6 – Phase 2: Identified Hazards
The SRM Panel identifies hazards as a collaborative effort. The tool(s) and technique(s) used to identify hazards should be specified and discussed. In this section, the identified hazards are documented, as well as their corresponding causes, the corresponding system states considered, and the consequent potential outcome. It is important to realize that while identification of the "worst credible outcome" and the system state in which the worst credible outcome occurs is required, system states with less severe outcomes should not be ignored. The information provided in this section should meet the requirements outlined in Chapter 3, Section 3.8 of the *ATO SMS Manual, Version 2.1*.

Section 7 – Phase 3 & 4: Risk Analysis & Risks Assessed
Describe the process used to analyze the risks associated with the identified hazards, referencing the Severity Definitions in Table 3.3 and the Likelihood Definitions in Table 3.4. Specify what type of data was used to determine likelihood of risk occurrence (e.g., quantitative or qualitative), as well as the sources of the data. The Risk Matrix should provide an illustration of the predicted initial/current risk(s) associated with the identified hazards. The information provided in this section should meet the requirements outlined in Chapter 3, Sections 3.9 - 3.10 of the *ATO SMS Manual, Version 2.1*.

Section 8 – Phase 5: Treatment of Risks/Mitigation of Hazards
If the existing controls and mitigations do not acceptably mitigate the hazards, then additional recommended safety requirements should be identified. It should reflect how the recommended safety requirements are expected to reduce the initial/current risk to an acceptable predicted residual risk level. Low risk hazards might still warrant recommended safety requirements. Ensure that the authority responsible for implementation of the recommended safety requirement(s) is aware of the requirement and was/is involved in the safety analysis. Moreover, should a mitigation require approval, then it is important to state this, as well as who

would be the approving authority. Risk mitigations are validated and verified prior to seeking SRMD approval. The information provided in this section should meet the requirements outlined in Chapter 3, Sections 3.11 of the *ATO SMS Manual, Version 2.1*.

Section 9 – Tracking and Monitoring of Hazards
Once the change/procedure has been approved and implemented, tracking of hazards and verifying the effectiveness of mitigation controls throughout the lifecycle of the system or change is required. Outline the methodology for this tracking and monitoring in this section. The information provided in this section should meet the requirements outlined in Chapter 3, Sections 3.11.11 - 3.11.13 of the *ATO SMS Manual, Version 2.1*.

APPENDICES

Appendix X – FAA Documents Related to the <proposed change name> SRMD – A listing of documents (orders, directives, regulations, handbooks, and manuals) that pertain to the proposed change, which have been consulted in the development of the proposed change and the corresponding safety analysis.

Appendix Y – Hazard Identification Tools – Provide information on the different tool(s), method(s), and technique(s) used during the safety analysis.

Appendix Z – Hazard Analysis and Risk Matrix – Depending on the analyses necessary, there might be one or more appendices with analyses. A risk matrix reflecting the initial and predicted residual risks should also be included.

Glossary – Acronyms and definitions for any terms listed in the SRMD.

Appendix K – SRMD Template

< proposed change name >
Safety Risk Management Document (SRMD)

<Suggestion: Insert screen-shot from modeling software or otherwise graphical depiction of proposed change, submitted for approval.>

NOTE 1:	**This generic SRMD provides guidance with regards to required information for an SRMD, though it should be tailored to the specific proposed change and the corresponding documentation needs.**
NOTE 2:	**New system acquisitions that are subject to the FAA Acquisition Management System (AMS) should use the Safety Risk Management Guidance for System Acquisitions (SRMGSA) for guidance in preparing the SRMD.**

Version 2.1

April 2008

SRMD Change Page

< A table will list changes made to the latest SRMD, the date and the version number >

Signature Page

Title: "< *proposed change name* > Safety Risk Management Document (SRMD)."

Initiator:
Initiator's Organization:
Initiator's Phone Number:

Submission Date:
SRMD #:
SRMD Revision Number:
SRMD Revision Date:

SRMD Approval Signature(s):
< Table 3.7 in the ATO SMS Manual, Version 2.1, provides guidance regarding who is to approve the SRMD. >

Signature	Name & Organization	Date
Signature	Name & Organization	Date

Risk Acceptance Signature(s):
< Table 3.8 in the ATO SMS Manual, Version 2.1, provides guidance regarding risk acceptance requirements. >

Signature	Name & Organization	Date
Signature	Name & Organization	Date

Proposal Rejection:
< If a proposed change is considered unsafe for implementation, such a decision should be recorded in the SRMD, with accompanying motivation. >

Signature	Name & Organization	Date
Signature	Name & Organization	Date

Executive Summary

< Provide a general descriptive summary of the proposed change/procedure, including a list of the dominant hazards and their corresponding predicted residual risk.
Summarize how the SRMD was developed and what process/method was used to move through the SRM process. E.g. whether it was the SRM process (as outlined in the SMS Manual) itself or that a proven process/method has been modified to make sure all SMS requirements are met. >

Table of Contents

SRMD Change Page **K-2**

Signature Page **K-3**

Summary **K-4**

Table of Contents **K-5**

List of Tables **K-6**

List of Figures **K-6**

Introduction **K-6**

Section 1 – Current System (System Baseline) **K-6**

Section 2 – Proposed Change **K-6**

Section 3 – Safety Risk Management Planning and Impacted Organizations **K-6**

Section 4 – Assumptions **K-7**

Section 5 – Phase 1: System Description **K-7**

Section 6 – Phase 2: Identified Hazards **K-7**

Section 7 – Phase 3 & 4: Risks Analysis & Risks Assessed **K-8**

Section 8 – Phase 5: Treatment of Risks / Mitigation of Hazards **K-12**

Section 9 – Tracking and Monitoring of Hazards **K-13**

APPENDICES ..... **K-**Error! Bookmark not defined.

Appendix J-A – FAA Documents Related to the *<proposed change name>* SRMD **K-14**

Appendix J-X – Hazard Identification Tools **K-14**

Appendix J-XX – Hazard Analysis and Risk Matrix **K-15**

Glossary **K-15**

List of Tables

< List of all tables (table # and name) presented in this document and their reference page. >

List of Figures

< List of all figures (figure # and name) presented in this document and their reference page. >

Introduction

< Provide a brief reasoning/motivation for the change/procedure initiative. The scope of the change, i.e., whether it concerns a local or a NAS wide proposed change, will affect the specific reasons for proposing a change. E.g., increased airport capacity through operational efficiency; reduction in airborne and ground delays; and reduction in fuel costs due to procedure efficiency. The originator should be identified in this section. >

Section 1 – Current System (System Baseline)

< Provide a description of the current system or existing procedures, as well as corresponding (operational) system states. If the proposal entails a procedural change, describe the current procedure and its operational environment. If the current system or procedure is unique and has challenges associated with its unique situation, be sure to point these out (E.g. Nation's capital – P56). It is also essential to address any planned future configuration, system or procedural changes that might affect the proposed change/procedure. >

Section 2 – Proposed Change

< Describe the proposed change/procedure, identifying which critical safety parameters are involved (E.g. prohibited/restricted airspace; noise abatement area; operational limitation; etc). Briefly introduce the types of verifications that will be performed throughout the development process to review whether the finalized proposed change will be safe, operational, and effective once implemented. Evaluation can consist of simulator modeling, live testing, or a combination thereof. If possible, provide a depiction of the proposed change/procedure. Be sure to also address the monitoring methods that will be used to verify system performance post-implementation. >

Section 3 – Safety Risk Management Planning and Impacted Organizations

< Before the SRM Process can begin, SRM planning is necessary. It is essential to select the appropriate SRM participants, schedule milestones, and assign tasks and responsibilities, etc. This will provide insight into how the SRM Process will be worked through as a team. If there is an existing process, which has been successfully used to develop and implement earlier systems, procedures, or changes, then please provide insight into how this process relates to the SRM and, if necessary, how this process was modified to ensure all SRM requirements were met.

With regards to the organizations that are impacted by the change, please describe the method used for collaboration during the identification, mitigation, tracking, and monitoring of hazards. While during the development of the change/procedure something might have seemed obvious to those involved, it might not be such an obvious decision choice to those reviewing the procedure at a (much) later time. Given this, describe how you have/will document the changes during procedure development phase.

Note: This section could reference one of the appendices, which would outline in more detail the current existing process, as well as any tools/methods/techniques/etc. used during initial change/procedure development. >

Section 4 – Assumptions

< If in the process of modifying an existing system or developing a procedure any assumptions are made in order to make the evaluation of the change more manageable, they are to be clearly defined and documented.

Moreover, if during the development process modeling tools are used, it is important to not only identify those tools, but also identify their limitations. E.g. If software is used, the software itself might have limitations. >

Section 5 – Phase 1: System Description

< The 'system description' should provide a description of the system/procedure, its operational environment, the people involved/affected by the change/procedure, the equipment required to accommodate the change/procedure, etc.

The 5M model, as described in the ATO SMS Manual, can be used as a reference to assist in ensuring that all necessary and relevant information is captured in the system description.

When describing the system, gathering any relevant available data with regards to the identified system elements and/or operational environment is necessary as it will help in analyzing the likelihood of risk occurrence (see Section 7). >

Section 6 – Phase 2: Identified Hazards

< Hazard identification is accomplished as a collaborative effort by core participants in the SRM process, although core participants are encouraged to consult with their colleagues throughout the hazard identification phase. In this section, you should identify and discuss the tool(s) and technique(s) used to identify hazards, listing at the top the hazards that turned out to be those of greatest concern, but not discounting the lesser hazards.

The ATO SMS Manual, Version 2.1, Appendix G provides a variety examples. It is not uncommon that a variety of tools/methods/techniques/etc. be used concurrently.

Some general sources *of hazards (from which specific hazards could be identified) could be as follows:*

- *Equipment (Hardware/Software)*
- *Operating environment*
- *Human operator*
- *Human machine interface*
- *Operational and maintenance procedures*
- *External services*
- *External service failures*

In summary, in the identify hazards section the identified hazards are to be documented, as well as their corresponding causes, the corresponding system states considered and the consequent potential outcome. It is important to realize that while identification of the "worst credible outcome" and "worst credible system state" is required, less severe outcomes and system states cannot be ignored. If it is known what time a system is in a certain system state, then this valuable data would assist in the understanding of the likelihood of risk occurrence (see Section 7). >

Section 7 – Phase 3 & 4: Risks Analysis & Risks Assessed

< Describe the process used to analyze the risks associated with the Section 6 – Phase 2 identified hazards, referencing the Severity Definitions in Table 7.1 (which row(s) was/were used?) and what types of quantitative data (e.g. data extracted from records or data based on calculated prediction) or qualitative data (e.g. expert judgment) were used to determine likelihood of risk occurrence.

When categorizing the severity of possible effect(s) of the respective hazards (using Table 7.1 – Severity Definitions), one should not consider the likelihood of that/those effect(s) occurring. Though, existing controls or requirement that would reduce the possibility of such an effect from occurring or reduce the likelihood of the hazard(s), are to be taken into account when determining the likelihood(s) of the effect(s). The likelihood is determined/estimated using Table 7.2 – Likelihood Definition (what column(s) was/were used?). It is not necessary to include Tables 7.1 and 7.2 in the SRMD. They are included in this template for reference. The same applies to the Risk Matrix. The SRMD must state the risk level associated with each hazard, but it is not necessary to show the hazards plotted in a diagram.

The estimated initial/ current risk can then be listed, as well as plotted in Figure 7.1 - Risk Matrix. The Risk Matrix will then provide an illustration of the predicted initial/current risk(s) associated with the identified hazards. >

Table 7.1: Severity Definitions

Effect On: ↓	Hazard Severity Classification				
	Minimal **5**	**Minor** **4**	**Major** **3**	**Hazardous** **2**	**Catastrophic** **1**
ATC Services	Conditions resulting in a minimal reduction in ATC services, or a loss of separation resulting in a Category D Runway Incursion(RI)[1], or proximity event	Conditions resulting in a slight reduction in ATC services, or a loss of separation resulting in a Category C RI[1], or Operational Error (OE)[2]	Conditions resulting in a partial loss of ATC services, or a loss of separation resulting in a Category B RI[1], or OE[2]	Conditions resulting in a total loss of ATC services, (ATC Zero) or a loss of separation resulting in a Category A RI[1] or OE[2]	Conditions resulting in a collision between aircraft, obstacles or terrain
Flight Crew	– Flightcrew receives TCAS Traffic Advisory (TA) informing of nearby traffic, or, – PD where loss of airborne separation falls within the same parameters of a Category D OE [2] or proximity Event – Minimal effect on operation of aircraft	-Potential for Pilot Deviation (PD) due to TCAS Preventive Resolution Advisory (PRA) advising crew not to deviate from present vertical profile, or, -PD where loss of airborne separation falls within the same parameters of Category C (OE) [2] *, or* -Reduction of functional capability of aircraft but does not impact overall safety e.g. normal procedures as per AFM	-PD due to response to TCAS Corrective Resolution Advisory (CRA) issued advising crew to take vertical action to avoid developing conflict with traffic, or, -PD where loss of airborne separation falls within the same parameters of a Category B OE [2], or, -Reduction in safety margin or functional capability of the aircraft, requiring crew to follow abnormal procedures as per AFM	-Near mid-air collision (NMAC) results due to proximity of less than 500 feet from another aircraft or a report is filed by pilot or flight crew member that a collision hazard existed between two or more aircraft -Reduction in safety margin and functional capability of the aircraft requiring crew to follow emergency procedures as per AFM	-Conditions resulting in a mid-air collision (MAC) or impact with obstacle or terrain resulting in hull loss, multiple fatalities, or fatal injury

Effect On: ↓	Hazard Severity Classification				
	Minimal **5**	**Minor** **4**	**Major** **3**	**Hazardous** **2**	**Catastrophic** **1**
Flying Public	– Minimal injury or discomfort to passenger(s)	– Physical discomfort to passenger(s) (e.g. extreme braking action; clear air turbulence causing unexpected movement of aircraft causing injuries to one or two passengers out of their seats) – Minor[3] injury to greater than zero to less or equal to 10% of passengers	– Physical distress on passengers (e.g. abrupt evasive action; severe turbulence causing unexpected aircraft movements) – Minor[3] injury to greater than 10% of passengers	Serious[4] injury to passenger(s)	Fatalities, or fatal[5] injury to passenger(s)

1 – As defined in 2005 Runway Safety Report
2 – As defined in FAA Order 7210.56, *Air Traffic Quality Assurance*, and N JO 7210.663*, Operational Error Reporting, Investigation, and Severity Policies*
3 – Minor Injury - Any injury that is neither fatal nor serious.
4 – Serious Injury - Any injury which: (1) requires hospitalization for more than 48 hours, commencing within 7 days from the date the injury was received; (2) results in a fracture of any bone (except simple fractures of fingers, toes, or nose); (3) causes severe hemorrhages, nerve, muscle, or tendon damage; (4) involves any internal organ; or (5) involves second- or third-degree burns, or any burns affecting more than 5 percent of the body surface.
5 – Fatal Injury - Any injury that results in death within 30 days of the accident.

Table 7.2: Likelihood Definitions

	NAS Systems & ATC Operational	NAS Systems		ATC Operational		Flight Procedures
		Qualitative				
	Quantitative	Individual Item/System	ATC Service/ NAS Level System	Per Facility	NAS-wide	
Frequent A	Probability of occurrence per operation/operational hour is equal to or greater than $1x10^{-3}$	Expected to occur about once every 3 months for an item	Continuously experienced in the system	Expected to occur more than once per week	Expected to occur more than every 1-2 days	Probability of occurrence per operation/operational hour is equal to or greater than $1x10^{-5}$
Probable B	Probability of occurrence per operation/operational hour is less than $1x10^{-3}$, but equal to or greater than $1x10^{-5}$	Expected to occur about once per year for an item	Expected to occur frequently in the system	Expected to occur about once every month	Expected to occur about several times per month	
Remote C	Probability of occurrence per operation/operational hour is less than or equal to $1x10^{-5}$ but equal to or greater than $1x10^{-7}$	Expected to occur several times in the life cycle of an item	Expected to occur numerous times in system life cycle	Expected to occur about once every year	Expected to occur about once every few months	Probability of occurrence per operation/operational hour is less than or equal to $1x10^{-5}$ but equal to or greater than $1x10^{-7}$
Extremely Remote D	Probability of occurrence per operation/operational hour is less than or equal to $1x10^{-7}$ but equal to or greater than $1x10^{-9}$	Unlikely to occur, but possible in an item's life cycle	Expected to occur several times in the system life cycle	Expected to occur about once every 10-100 years	Expected to occur about once every 3 years	Probability of occurrence per operation/operational hour is less than or equal to $1x10^{-7}$ but equal to or greater than $1x10^{-9}$
Extremely Improbable E	Probability of occurrence per operation/operational hour is less than $1x10^{-9}$	So unlikely that it can be assumed that it will not occur in an item's life cycle	Unlikely to occur, but possible in system life cycle	Expected to occur less than once every 100 years	Expected to occur less than once every 30 years	Probability of occurrence per operation/operational hour is less than $1x10^{-9}$

Severity / Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A					
Probable B					
Remote C					
Extremely Remote D					
Extremely Improbable E					*

* Unacceptable with Single Point and/or Common Cause Failures

High Risk
Medium Risk
Low Risk

Figure 7.1: Risk Matrix

Section 8 – Phase 5: Treatment of Risks / Mitigation of Hazards

< In some instances the existing controls and mitigations are sufficient in reducing the risk(s) associated with the identified hazards to an acceptable level. However, should they not be adequate then additional recommended safety requirements should be identified in this section. It should reflect how the recommended safety requirements are expected to reduce the initial/current risk to and acceptable predicted residual risk level. Low risk hazards might still warrant recommended safety requirements.

Section is to show what steps have been taken to reduce the estimated likelihood of the possible effect(s) from occurring, thus reducing the predicted residual risk. In identifying risk mitigations, it is important to identify who will be required to implement the mitigation. Meanwhile, this will provide a means to ensure that the authority responsible for implementation is aware of this requirement and was/is involved in the SRM process. Moreover, should a mitigation require approval, then it is important to state this, as well as who would be the approving authority. Note: Risk mitigations must be validated and verified prior to seeking SRMD approval. >

Section 9 – Tracking and Monitoring of Hazards

< Once a new change/procedure has been approved and implemented, it is essential to make sure the change/procedure does, in fact, function in the way for which it had been designed, and that the estimated risk(s) maintain reflective in the real-life environment. In this section, the methodology for tracking hazards and verifying effectiveness of mitigation controls throughout the lifecycle of the system or change should be outlined. Table 9.1 shows a sample recommended control implementation/monitoring plan structure that can be used.

Note: Hazard tracking is an essential element of SRM, which can be accomplished through the use of an automated system, as described in Chapter 3, Sections 3.11.11 – 3.11.13 of the ATO SMS Manual, Version 2.1. Also note that the hazard tracking system must be linked to operational metrics to verify that the risk mitigation strategies are effective in controlling the hazard. In this respect, it is often useful to develop safety performance indicators and targets. >

Table 9.1: Sample Recommended Control Implementation/ Monitoring Plan Structure

Task	Responsible	Due Date/ Frequency	Status
Implementation of Controls			
Monitoring			

Appendix K-A – FAA Documents Related to the *<proposed change name>* SRMD

The following list of documents (orders, directives, regulations, handbooks, and manuals) addresses NAS safety management that relates to *<proposed change name>* and has been consulted in the development of the *<proposed change name>* and the SRM Process. In some cases the document listed below may have been updated since this list was compiled. Please refer to the office of primary interest for the most recent version of the document.

For Example:

Required Navigation Performance:

- *Roadmap for Performance – Based Navigation, Evolution for Area Navigation (RNAV) and Required Navigation Performance (RNP) Capabilities, 2003-2020.*
- *Notice 8000.287, Airworthiness and Operational Approval for Special Required Navigation Performance (RNP) Procedures with Special Aircraft and Aircrew Authorization Required (SAAAR).*
- *…*

Airports:

- *…*

Air Traffic Control:

- *Order 7100.9, Standard Terminal Arrival (STAR)*
- *Order 7930.2, Notices to Airmen (NOTAMs)*
- *…*

Facilities & Equipment:

- *…*

Flight Procedures:

- *Order 8260.3B CHG 19, United States Standard for Terminal Instrument Procedures (TERPS)*
- *Order 8260.19C CHG 3, Flight Procedures and Airspace*
- *Order 8260.43A, Flight Procedures Management Program*
- *Order 8260.44, Civil Utilization of Area Navigation (RNAV) Departure Procedures*
- *Order 8260.46, Departure Procedures (DP) Program*
- *…*

Safety Risk Management:

- *Order 8040.4, Safety Risk Management*
- *ATO SMS Manual – Version 2.1*

Appendix K-X – Hazard Identification Tools

<Description/information on the different tool(s)/method(s)/technique(s) used during the SRM process. >

Appendix K-XX – Hazard Analysis and Risk Matrix

< Depending on the analyses necessary, there might be one or more appendices with analyses; a Risk Matrix reflecting the predicted residual risks is also to be included. >

Glossary

< Insert any acronyms listed in this document and provide definitions for any relevant terms. >

Appendix L – SRMD Review Checklist

Item #	SMS Manual Requirement	SMS Manual V2.1 Reference	Compliant?	Category	Remarks
TITLE AND SIGNATURE PAGE					
1	Is the document clearly titled?	Appendix J	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
2	Is the document appropriately dated?	Appendix J	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
3	Is the originator appropriately identified?	Appendix J	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
4	Did the appropriate individuals review the document?	3.13.2	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
5	Did the appropriate individuals approve the document?	3.13	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
6	Did the appropriate individuals accept the risk(s) outlined in the document?	3.14	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
7	Is AOV approval required?	3.4.4 – 3.4.6	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	

Item #	SMS Manual Requirement	SMS Manual V2.1 Reference	Compliant?	Category	Remarks
EXECUTIVE SUMMARY					
8	Does the executive summary include justification of the proposed change, a summary of the hazards and the corresponding initial and residual risks?	Appendix J	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
INTRODUCTION					
9	Does the document provide a brief reasoning or motivation for the change/procedure?	Appendix J	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
SECTION 1: CURRENT SYSTEM/BASELINE					
10	Does the document provide enough information about the present system to assess the impact of the change?	3.7	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
SECTION 2: PROPOSED CHANGE					
11	Does the document provide a clear description of the proposed change?	3.7 3.12.2	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
12	Was (the potential impact of) the proposed change appropriately bounded?	3.7.4 3.12.2	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
SECTION 3: SAFETY RISK MANAGEMENT PLANNING AND IMPACTED ORGANIZATIONS					
13	Were stakeholders appropriately involved/ consulted?	3.4.1 – 3.4.3 3.7.5	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	

Item #	SMS Manual Requirement	SMS Manual V2.1 Reference	Compliant?	Category	Remarks
SECTION 4: ASSUMPTIONS					
14	Were any relevant assumptions clearly defined and documented?	Appendix J	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
SECTION 5: SYSTEM DESCRIPTION					
15	Does the system description provide a description of the system/procedure, its operational environment, and the people involved/affected by the change/procedure, the equipment required to accommodate the change/procedure, etc.?	3.7.1	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
16	Is the proposed change a NAS-wide change?	3.7.2	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
SECTION 6: IDENTIFIED HAZARDS					
17	Were the identified hazards clearly documented?	3.8.4	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
18	Were the corresponding causes of the identified hazards clearly documented?	3.8.5	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
19	Were different system states considered in the evaluation of the identified hazards?	3.8.5	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	

Item #	SMS Manual Requirement	SMS Manual V2.1 Reference	Compliant?	Category	Remarks
SECTION 7: RISK ANALYSIS AND ASSESSMENT					
20	Were the severities of the identified hazards determined and was supporting rationale provided?	3.9.3	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
21	Were the likelihoods of outcomes of the identified hazards determined and was supporting rationale provided?	3.9.4	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
22	Were any relevant existing controls and mitigations clearly documented?	3.9.2	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
23	Were the residual risks of the identified hazards clearly documented?	3.10	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
24	Were the risks associated with the identified hazards appropriately categorized as high, medium, or low?	3.10	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
SECTION 8: TREATMENT OF RISKS/MITIGATIONS OF HAZARDS					
25	Were any relevant recommended safety requirements clearly documented?	3.11	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
26	Does the document contain draft LOAs, LOPs, SOPs, or NOTAMS if cited as a mitigation of risk?	3.12.2	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	

Item #	SMS Manual Requirement	SMS Manual V2.1 Reference	Compliant?	Category	Remarks
27	If risk was transferred to another party, was their assumption of that risk documented?	3.11.5	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
SECTION 9: TRACKING AND MONITORING OF HAZARDS					
28	Was an implementation plan included in the document?	3.11.13	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
29	Was a description of a method for tracking hazards, verifying effectiveness of mitigation controls, and monitoring operations data included in the document?	3.11.11 – 3.11.13 3.12.2	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
MISCELLANEOUS					
30	Are appendices for references appropriately included?	Appendix J	☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	
31	Are there any additional (general) comments?		☐ Yes ☐ No ☐ N/A	☐ Mandatory ☐ Administrative ☐ Suggestion	

Appendix M – SRM and Operational Changes to the ATC System

1. Applying SRM to ATC Operations Changes

As Chapter 3, *Safety Risk Management*, discusses, the SMS and its processes apply to changes to ATC procedures and standards, equipment or facilities, airspace, airport procedures, new systems, and modifications to existing systems (hardware, software, and any corresponding procedures).

The implementation of operational changes (e.g., new or modified ATC procedures, airspace changes, new or modified maintenance procedures) often has the potential for a negative impact to safety. Personnel assess each of these changes for acceptable safety risk prior to implementation of a change. Within the context of the SMS, personnel accomplish this assessment though SRM, which requires that they assess intended changes for risk in the analysis and planning phases of changes and, certainly, before implementation.

The fundamental process for assessing the risk associated with operational changes is essentially the same as that for engineering/ system acquisition-type changes. Personnel follow the five-phase process discussed in Chapter 3, *Safety Risk Management*. This section offers additional guidance related specifically to the assessment of operational changes, which are often best assessed using a panel of Subject Matter Experts (SMEs) to collect hazard and error data, identify the hazards, analyze and calculate their risk, and develop mitigation strategies.

2. SRM Panel Expertise

An SRM Panel conducts a safety analysis of ATC operational changes, as Chapter 3, *Safety Risk Management,* (Section 3.4) describes. The make-up of the panel will vary with the type and complexity of the change; personnel should give consideration to including the following expertise on the SRM Panel:

- ATC personnel directly responsible for procedure design
- ATC personnel with current knowledge and experience of the procedural area under assessment (i.e., system users)
- Hardware and/or software engineering or automation expert to provide knowledge on equipment performance
- Second-level engineering support for the equipment or software
- Safety risk management specialist to guide the application of the methodology
- Human Factors specialist
- Software specialist
- Systems specialist
- Personnel with skill in the collection and analysis of hazard and error data, and in the use of specialized tools and techniques (e.g., operations research analysts, data analysts, Human Factors analysts, and failure mode analysts)

3. Steps Used to Assess an ATC Procedural Change

Risk assessment of operational changes typically involves the following steps:

Step 1. Identify what the change involves (e.g., a control procedure, change in equipment, maintenance procedure, etc). There are times when a change could involve more than one. For instance, an equipment change is often accompanied by procedural changes.

Step 2. Break down the change(s) into manageable components. For example, one might divide control procedures into:

- Transfer of control procedures
- Coordination procedures
- Radar procedures
- Holding procedures
- Speed control procedures
- Runway procedures

One might divide equipment procedures into:

- Set-up procedures
- Operations under normal and emergency conditions
- Operations under equipment failure or partial failure conditions

Step 3. Identify potential hazards that affect the ability to maintain safe separation and/or the safety of the NAS. Personnel best achieve this by evaluating task performance through data collection and analysis, and through user inquiry to determine "What can go wrong?" and "What if...?" in relation to the identified divisions in Step 2. Other tools that may be appropriate for personnel to use in assessing operational changes are the Human Error Analysis and the Scenario Analysis. (Information on these and other hazard identification tools can be found in Appendix G, *Hazard Identification and Analysis Tools and Techniques*.)

Step 4. The group assesses the hazard severity as Table 3.3 describes.

Step 5. The group identifies the circumstances or incident sequence under which a hazard might occur and the likelihood of occurrence, as Table 3.4 describes.

Step 6. The group examines the hazard and incident analysis and identifies risk mitigation measures where necessary. More information on risk mitigation can be found in Chapter 3, *Safety Risk Management*, Section 3.11.

Step 7. Personnel generate an SRMD and get the appropriate approval and risk acceptance as described in Chapter 3, *Safety Risk Management*.

Appendix N – Deployment Planning Process with SRM

The Deployment Planning Process is part of the ATO's continuing efforts to deliver updated, operationally ready air traffic systems (hardware/software) and services to the field. The Deployment Planning Process and the In-Service Decision (ISD) are part of AMS and are usually associated with the acquisition or modification of NAS systems.

The ISD Secretariat, who is responsible for managing the Deployment Planning Process for the ATO, is now included within ATO Safety Services. This ensures that the implementing service organizations give the appropriate attention to the safety-related aspects of developing new systems or modifying existing systems.

Deployment Planning Process activities are grouped into five phases that parallel acquisition management lifecycle activities: Investment Analysis, Early Solution Implementation, Pre-ISD, ISD, and Post-ISD.

During Investment Analysis, the Deployment Planning Process focuses on the development of an In-Service Review (ISR) checklist for use in program planning and requirements definition. The template for this checklist was modified to include SRM-related requirements, the Program Safety Plan, use of HTS, the System Safety Assessment Report (SSAR), and verification of safety requirements. Stakeholders from relevant organizations also participate in the planning process. During Early Solution Implementation, a program's ISR checklist with its safety requirements is reviewed regularly with stakeholders to monitor progress and document the completion of various tasks. In addition, an SRMD is completed prior to proceeding to an ISD.

For Pre-ISD activities, all program stakeholders, including those with safety-related interests, are actively involved with ISD readiness reviews. ISD activities involve meetings at the ATO Vice President level (including the Vice President of ATO Safety Services) and above. Action Plans for outstanding issues, including safety issues, are presented at these meetings for approval. For Post-ISD activities, the ISD Secretariat tracks any outstanding issues by using an action plan tracking system.

Figure N.1 summarizes the integration of the Deployment Planning Process with SRM.

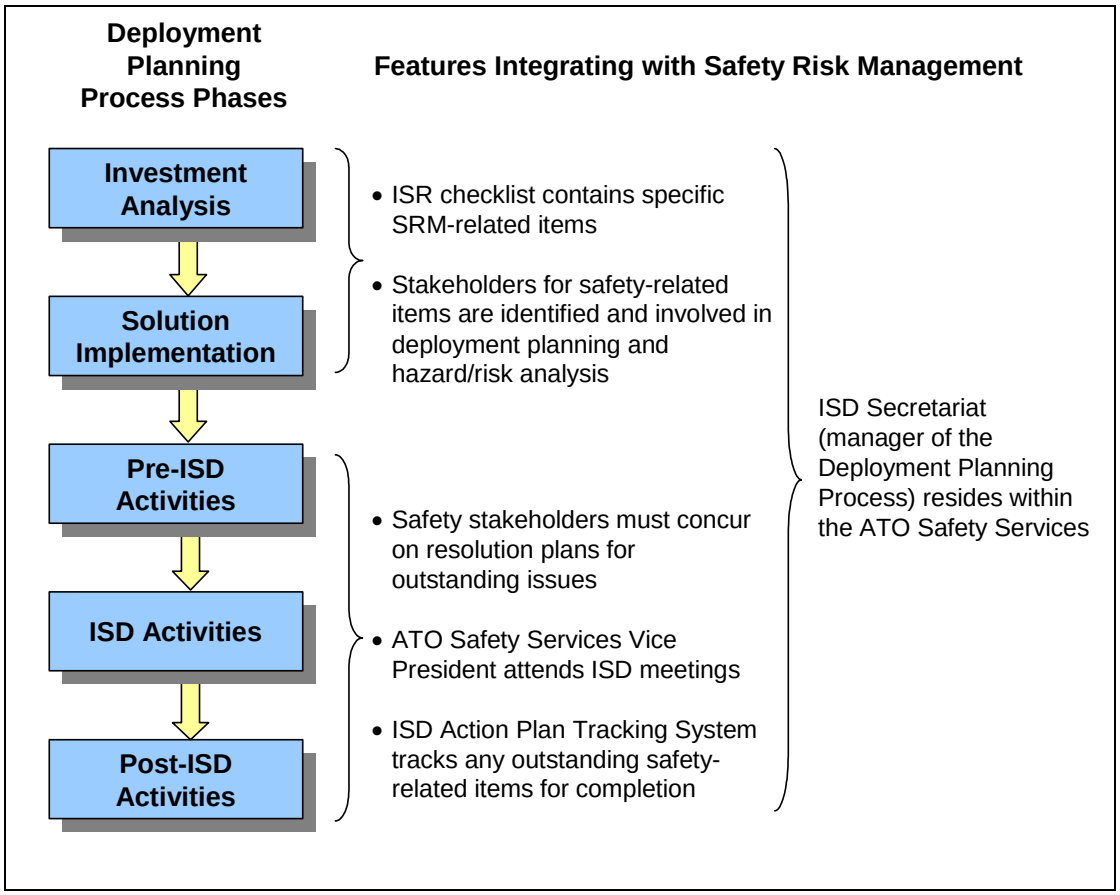


Figure N.1: Integration of the Deployment Planning Process with SRM

SRM Lifecycle

The SRM lifecycle organizes a series of phases and decision points as shown in Figure N.2. The circular representation conveys the principle of integrated management and continuous improvement in service delivery over time. Application is flexible and may be tailored as appropriate dependent upon the scope and depth of the NAS change.

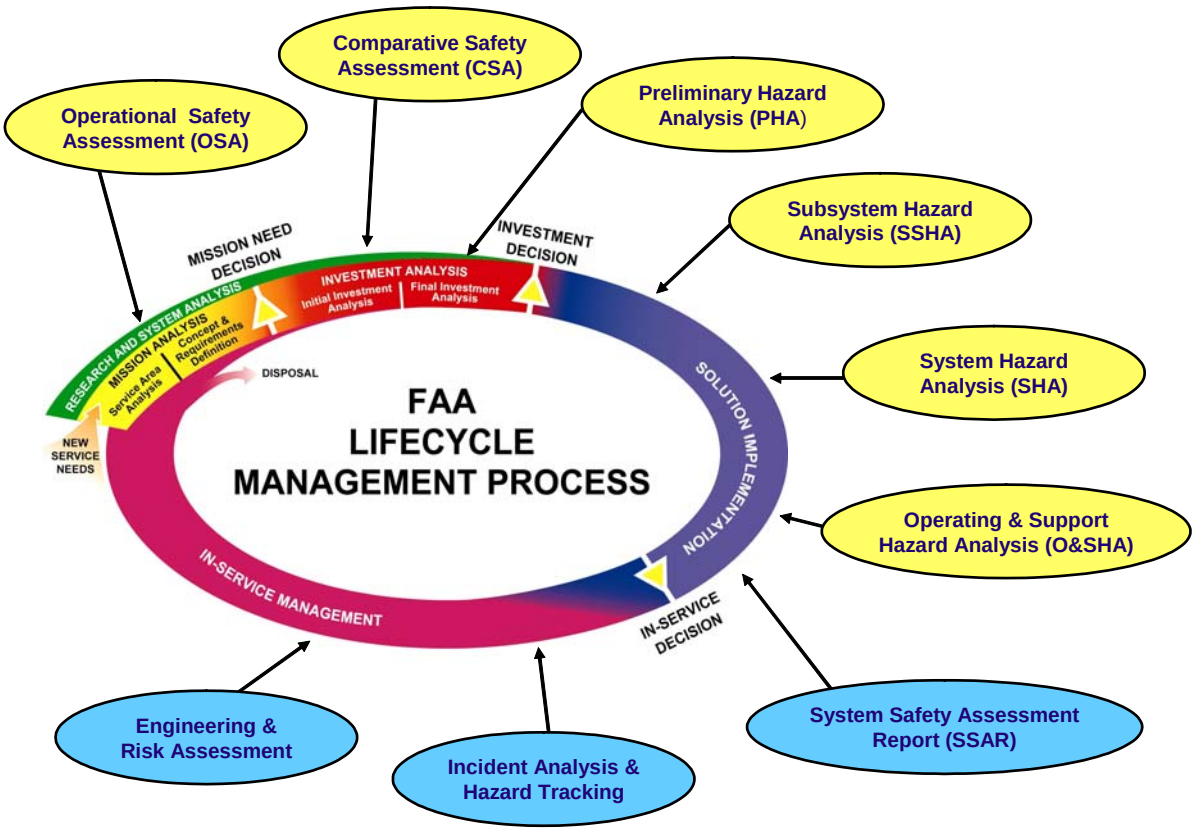


Figure N.2: Lifecycle Management and SRM Process