Safety Management System Manual
July 2026

Air Traffic Organization

ALL POINTS/SAFETY
everyone. everywhere. everyday.

FAA
Air Traffic Organization

Contents

1.1 About the Safety Management System Manual

The Air Traffic Organization (ATO) Safety Management System (SMS) is a formalized and proactive approach to system safety. It directly supports the mission of the Federal Aviation Administration (FAA): "to provide the safest, most efficient aerospace system in the world." The ATO **SMS** is an integrated collection of policies, processes, procedures, and programs used to manage safety risk in the provision of air traffic management and communication, navigation, and surveillance services.

The ATO SMS Manual informs ATO employees and contractors about the goal of the ATO SMS, describes the interrelationship among the four components of the SMS, and instructs readers on the process of identifying safety hazards and mitigating risk in the National Airspace System (NAS). More detailed guidance on the practical application of the SMS, and specifically Safety Risk Management (SRM), is contained in the annex of this document. This SMS Manual and its complements, such as the Safety Risk Management Guidance for System Acquisitions (SRMGSA), ATO Safety Guidance documents, and other FAA safety documents, are used to carry out the safety mission of the FAA and requirements of the SMS.

1.1.1 Changes to the SMS Manual

Safety (AJI) reviews this SMS Manual annually. Individuals who would like to propose a change to the document may submit comments via the ATO SMS Policy Management Portal.

1.2 Establishment and Continuous Support of the ATO SMS

Safety, the principal consideration of all ATO activities, is defined as the state in which the risk of harm to persons or damage to property is acceptable. Managing and assuring the safety of operations using the SMS has long been a focus of air navigation service providers worldwide, with the International Civil Aviation Organization (ICAO) having provided the guiding principles and the mandate for member organizations to use an SMS. The ATO's SMS efforts support the FAA safety mission, which emphasizes continuous improvement of safety and the integration of safety management activities across FAA organizations, programs, and Lines of Business (LOBs). Efforts to develop and implement complex, integrated Next Generation Air Transportation System systems to improve the safety and efficiency of air travel in the United States make clear the relevance of the SMS.

1.3 SMS Policy Derivations

The ATO SMS is supported by numerous levels of policy and requirements, as depicted in Figure 1.1. Relevant programs that predate the SMS are detailed in other FAA publications and processes. This SMS Manual only references those documents when necessary. Section 1.8 lists many of the related documents.

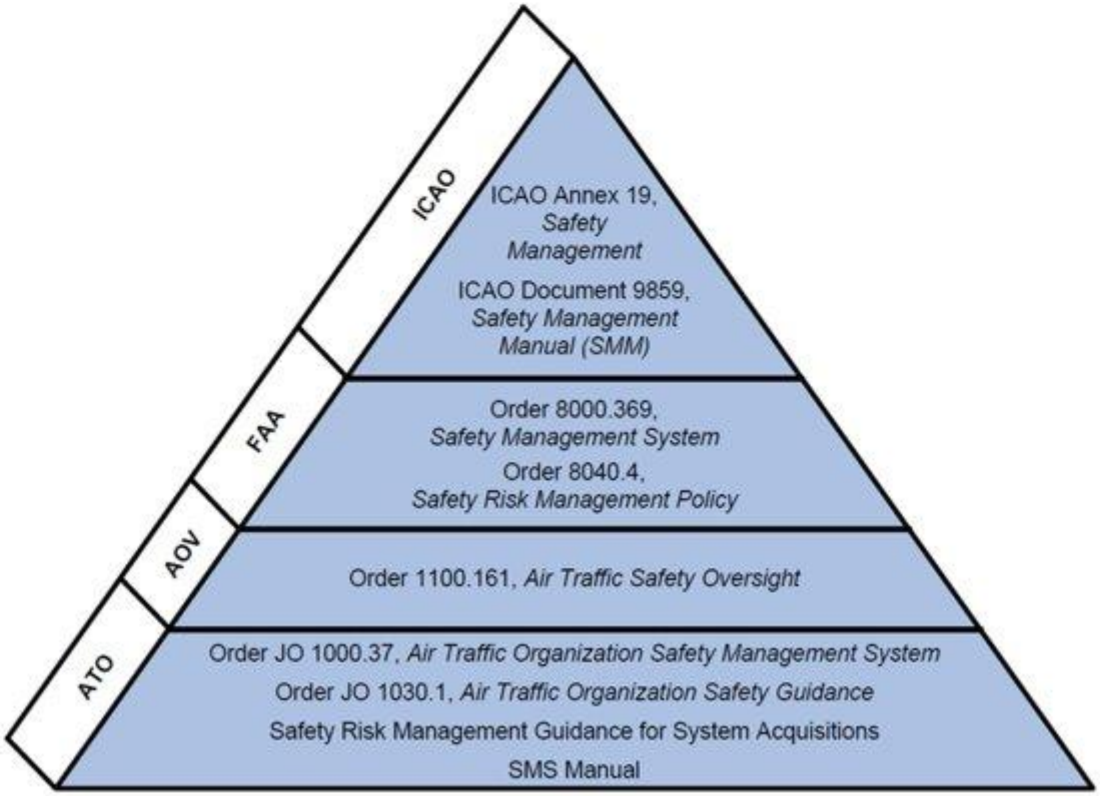


Figure 1.1: SMS Policy and Requirements Hierarchy

1.3.1 ICAO SMS Policy

The FAA derives its high-level SMS policy from ICAO policy. ICAO Annex 19, *Safety Management*, provides standards and recommended practices for safety management for member states and air traffic service providers. Additionally, ICAO Document 9859, *Safety Management Manual (SMM)*, provides guidance for the development and implementation of the SMS for air traffic service providers. ICAO Document 9859 also provides guidance for safety programs in accordance with the international standards and recommended practices contained in Annex 19.

1.3.2 FAA SMS Policy

FAA Order 8000.369, *Safety Management System*, describes the essential aspects of an SMS and provides implementation guidance to FAA organizations. This document is designed to create a minimum SMS standard that each FAA LOB can follow to implement an SMS.

FAA Order 8040.4, *Safety Risk Management Policy*, establishes requirements for how to conduct SRM in the FAA. It formalizes SRM guidance for FAA LOBs and Staff Offices and describes specific steps when performing and documenting SRM that crosses FAA LOBs. The ATO must consider and, when necessary, use the provisions in this order when coordinating SRM with other FAA organizations. AJI functions as the ATO liaison to interface with outside organizations. Within the ATO, AJI adjudicates discrepancies among Service Units.

1.3.3 Air Traffic Safety Oversight Service Order

The Air Traffic Safety Oversight Service (AOV) provides independent safety oversight of the ATO. FAA Order 1100.161, *Air Traffic Safety Oversight*, provides high-level SMS requirements of the ATO and AOV. When AOV involvement is required, AJI functions as the liaison between AOV and other ATO Service Units and organizations. Additional guidance from AOV is submitted via Safety Oversight Circulars (SOCs) that provide information that may be used by the ATO to develop and implement internal procedures. AOV publishes all SOCs on the intranet.

1.3.4 ATO SMS Policy and Requirements

FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*, documents high-level SMS requirements, roles, and responsibilities. FAA Order JO 1030.1, *Air Traffic Organization Safety Guidance*, establishes a method and process for providing the ATO with supplemental guidance material pertinent to the SMS. The SRMGSA provides SMS requirements and guidance pertinent to programs proceeding through the FAA Acquisition Management System (AMS) process. The ATO has also established Quality Assurance and Quality Control orders that govern safety data collection and the establishment of safety-related corrective actions. Those orders are as follows:

- FAA Order JO 7210.632, *Air Traffic Organization Occurrence Reporting*
- FAA Order JO 7210.633, *Air Traffic Organization (ATO) Quality Assurance (QA)*
- FAA Order JO 7210.634, *Air Traffic Organization (ATO) Quality Control*
- FAA Order JO 7200.20, *Voluntary Safety Reporting Programs*

All ATO organizations and individuals under the purview of FAA Order JO 1000.37 must adhere to the provisions of the aforementioned documents and this SMS Manual. If discrepancies exist between this SMS Manual and FAA orders and guidance, including those that originate outside the ATO, notify the Safety Management Group, AJI-31, Manager via the ATO SMS mailbox.[1]

1.4 The Four Components of SMS

There are four components of the SMS that combine to create a systematic approach to managing and ensuring safety. These components are:

- **Safety Policy:** The documented organizational policy that defines management's commitment, responsibility, and accountability for safety. Safety Policy identifies and assigns responsibilities and accountabilities to key safety personnel.
- **SRM:** A process within the SMS composed of the following steps: describing the system; identifying the hazards; and analyzing, assessing, and treating risk. SRM includes requirements for defining monitoring strategies for the identified safety risk of the NAS.
- **Safety Assurance:** A set of processes within the SMS that verify that an organization meets or exceeds its safety performance objectives. These processes function systematically to determine the effectiveness of safety risk controls through the collection and analysis of data and assessment of information.

1. The role of the AJI-31 Group Manager is defined in FAA Order JO 1000.37.

- **Safety Promotion:** The communication and distribution of information to improve the safety culture and the development and implementation of programs and/or processes that support the integration and continuous improvement of the SMS within the ATO. Safety Promotion allows the ATO to share and provide evidence of successes, best practices, and lessons learned.

Figure 1.2 represents the relationship of the four SMS components in an integrated model. The integration and interaction of the four components is essential to managing the SMS effectively and fostering a positive safety culture.

Figure 1.2: The Integrated Components of the SMS

1.4.1 Safety Culture and Promotion in the ATO

Safety culture is defined as an organization's shared actions, values, and behaviors—modeled by its leaders and internalized and acted upon by its members—that demonstrate a commitment to safety over competing goals and demands. All levels of management must actively promote and provide leadership to foster a mature and positive safety culture. The ATO uses its SMS to promote a positive safety culture through policies that align safety goals with organizational standards, training, voluntary reporting, and best practices. A strong safety culture helps ensure that personnel are trained and competent to perform their duties and that continual updates on training are provided. The ATO's safety culture is underpinned by five supporting elements: a just culture, a flexible culture, an informed culture, a reporting culture, and a learning culture.

Promoting strong safety values means that all ATO employees share lessons learned from investigations (as authorized) and experiences, both internally and from other organizations. Safety Promotion programs and activities are vital to achieving positive safety outcomes throughout the ATO. The tenets of Safety Promotion are used to foster a positive safety culture in which ATO employees understand why safety is important and how they affect it, providing a sense of purpose to safety efforts. Each employee must consider the potential effect that their decisions may have on safety, and each employee is responsible for understanding the significance of their job as it relates to safety. SMS training identifies the importance of the SMS and how each employee and contractor fits into the mission of using the SMS to improve safety in the ATO. For more information on SMS training, refer to the ATO SMS Toolbox.

Open communication is critical to a positive safety culture. The ATO communicates safety objectives to all operational personnel to improve the way safety is perceived, valued, and prioritized. In an organization with a strong safety culture, individuals and groups take responsibility for safety by communicating safety concerns and striving to learn, adapt, and modify individual and organizational behavior based on lessons learned. For more information on Safety Culture and its constituent elements, refer to the Safety Culture page on the ATO SMS Toolbox.

1.4.1.1 Safety Programs and Initiatives

The ATO maintains a positive safety culture using programs and initiatives such as:

- **Recurrent Training:** An initiative that uses collaboratively developed instruction designed to maintain and update previously learned skills while promoting a positive safety culture.
- **Fatigue Risk Management:** A group that provides operational fatigue risk expertise, guidance, and support to the ATO in developing fatigue reduction strategies and policy recommendations to mitigate and manage operational fatigue risks in the NAS.
- **Partnership for Safety:** A joint effort between the ATO and the National Air Traffic Controllers Association that encourages employees to become actively engaged in identifying local hazards and developing safety solutions before incidents occur.
- **Voluntary Safety Reporting Programs**
    - **Air Traffic Safety Action Program (ATSAP):** A confidential system for controllers and other employees to voluntarily identify and report safety and operational concerns. For more information, refer to the ATSAP website.
    - **Confidential Information Share Program (CISP):** A program for the sharing and analysis of information collected through the ATSAP and airlines' Aviation Safety Action Programs to provide a more complete representation of the NAS. For more information, visit the CISP website.
    - **Technical Operations Safety Action Program (T-SAP):** A system for reporting safety-related events or issues pertaining to operations, equipment, personnel, or anything believed to affect safety in the NAS for technicians and other Technical Operations employees. For more information, refer to the T-SAP website.
- **Change Advisory Group:** A group that promotes open communication with ATO SMS stakeholders and affected organizations by providing an effective and efficient policy revision process and expediting the review and concurrence process for the ATO SMS Manual.
- **Runway Safety:** A team that works with all stakeholders to develop innovative programs and techniques to reduce the severity and likelihood of surface incidents.

- **Lessons Learned:** An initiative that improves ATO processes, addresses deficiencies proactively, and empowers employees to play a direct role in the safety of the NAS by providing valuable safety information.

1.5 SMS Benefits

ATO processes and tools that support the SMS help:

- Provide a common framework to proactively and reactively identify and address safety hazards and risks associated with NAS equipment, operations, and procedures;
- Encourage intra-agency stakeholders to participate in solving the safety challenges of an increasingly complex NAS;
- Reduce isolated decision-making by using integrated safety management principles;
- Improve accountability for safety through defined managerial roles and responsibilities and SRM processes;
- Integrate Safety Assurance processes that enable the ATO to effectively measure safety performance;
- Provide documentation of the ATO’s data-based efforts to improve NAS safety using a repeatable process;
- Promote a continuous cycle of assessing, correcting/mitigating, and monitoring the safety of air navigation services;
- Foster a positive safety culture that can help improve system safety; and
- Measure the performance and support the improvement of the SMS.

1.6 SMS Continuous Improvement

The SMS is the framework that the ATO uses to measure and help ensure the safety of its operations. In an evolving NAS, it is necessary to continuously seek improvement in ATO processes and policies that support ATO safety efforts and, by extension, support the SMS. The ATO and external organizations conduct audits/assessments to measure and determine compliance with the policies and procedures for managing safety in the NAS. By assessing SMS maturity, the ATO is able to identify gaps in SMS performance, opportunities for improvement, and areas in which to focus new policy development.

1.6.1 Measuring NAS-Wide ATO Safety Performance

Historically, the ATO has based the identification of risk on whether an operation was compliant or separation was maintained; however, this approach has not always identified all aspects of risk in the most effective manner. Similarly, compliant operations have, on occasion and under certain applications, introduced varying levels of risk into the NAS.

Moving forward, the ATO will rely more on risk-based safety data to identify and analyze safety issues and evaluate the effectiveness of safety risk mitigation. The ATO has adopted a risk-based approach to collecting and analyzing data, rather than gathering and evaluating data based solely upon existing compliance standards. Understanding the level of risk associated with an operation is a holistic safety method that can proactively look beyond compliance. Risk-based safety addresses shortcomings without the boundaries of traditional compliance-based analysis.

Further, when appropriate, risk-based data collection and analysis should utilize a common taxonomy. A common taxonomy ensures robust, consistent classification and analysis of safety trends; facilitates comparison of risk findings across SRM documents; and enables association of operational safety data and accident/incident investigation data with specific SRM efforts. Additionally, aligning risk-based data collection with a common taxonomy can help prevent inconsistent risk analysis across similar SRM efforts, facilitating effective, accurate, and comprehensive safety analyses.

1.7 Policy Compliance with SMS

As the ATO's SMS matures, the tenets of the SMS components are integrated into new and existing ATO policy. For a directive to be considered compliant with the SMS, it must incorporate safety measures and SMS requirements to help manage safety.

1.8 FAA Documents Related to SMS Requirements

The following documents (orders, directives, handbooks, and manuals) address NAS safety management and are core documents that support the ATO SMS. This list is not all-inclusive and only represents a small portion of ATO documents that pertain to safety management. Some documents listed may have been updated since the publication of this SMS Manual.

1.8.1 Safety Reporting

a. FAA Order 7050.1, *Runway Safety Program*
b. FAA Order JO 7200.20, *Voluntary Safety Reporting Programs*
c. FAA Order JO 7210.632, *Air Traffic Organization Occurrence Reporting*
d. FAA Order JO 7210.633, *Air Traffic Organization (ATO) Quality Assurance (QA)*
e. FAA Order JO 7210.634, *Air Traffic Organization (ATO) Quality Control*
f. FAA Order JO 8020.16, *Air Traffic Organization Aircraft Accident and Aircraft Incident Notification, Investigation, and Reporting*
g. FAA Order 8900.1, *Flight Standards Information Management System*

1.8.2 Facilities and Equipment Management

a. FAA Order JO 1320.58, *Instructions for Writing Notices, Maintenance Technical Handbooks, and System Support Directives*
b. FAA Order 1800.66, *Configuration Management Policy*
c. FAA Order JO 1900.47, *Air Traffic Control Operational Contingency Plans*
d. FAA Order 6000.15, *General Maintenance Handbook for NAS Facilities*
e. FAA Order 6000.30, *National Airspace System Maintenance Policy*
f. FAA Order JO 6000.50, *National Airspace System (NAS) Integrated Risk Management*

1.8.3 Hardware and Software System Development

a. FAA AMS
b. FAA Systems Engineering Manual

1.8.4 Safety Management and Risk Assessment

a. SRMGSA

b. AOV SOC 07-02, *AOV Concurrence/Approval at Various Phases of Safety Risk Management Documentation and Mitigations for Initial High-Risk Hazards*

c. AOV SOC 07-05A, *Guidance on Safety Risk Modeling and Simulation of Hazards and Mitigations*

d. AOV SOC 13-13A, *Corrective Action Plan Development and Acceptance in Response to Safety Compliance Issues*

e. FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*

f. FAA Order JO 2900.2, *Air Traffic Organization Audits and Assessments*

g. FAA Order 1100.161, *Air Traffic Safety Oversight*

h. FAA Order 8000.369, *Safety Management System*

i. FAA Order 8040.4, *Safety Risk Management Policy*

j. FAA Order 8040.6, *Unmanned Aircraft Systems Safety Risk Management Policy*

2.1 Introduction to Managing System Safety

As Air Traffic Organization (ATO) operational procedures and National Airspace System (NAS) equipment (i.e., hardware and software) evolve, their interaction and interdependency across organizations within the ATO and throughout the Federal Aviation Administration (FAA) must be addressed. In a system as large and diverse as the NAS, the identification of a safety hazard and mitigation of its risk often falls within the purview of multiple organizations.

The effects of safety hazards and associated risk management methods across multiple organizations, domains, and implementation timelines must be properly understood to achieve the highest practical level of safety. Safety risk deemed acceptable for an individual element of the NAS may lead to unintentional safety risk in another element if Safety Risk Management (SRM) is not conducted with a "system of systems" philosophy. As emerging NAS equipment, operations, and procedures are tested and implemented, the SRM process must account for their potential safety impact on existing/legacy tools and procedures and vice versa. Sharing safety data and using an integrated safety management approach helps identify and resolve issues requiring the consideration of multiple disciplines.

The goal of an integrated approach to safety management is to eliminate gaps in safety analyses by assessing NAS equipment, operations, and procedures across three planes: vertical, horizontal, and temporal. The vertical plane is hierarchical, providing assessments from a specific project up to the NAS-level system of systems of which the project is a part. The horizontal plane spans organizations, programs, and systems. Finally, the temporal plane attempts to eliminate safety gaps across program and system implementation timelines. Figure 2.1 depicts several factors in each of the three planes that should be considered to ensure an integrated approach to safety management. Refer to the Safety Risk Management Guidance for System Acquisitions for more information.

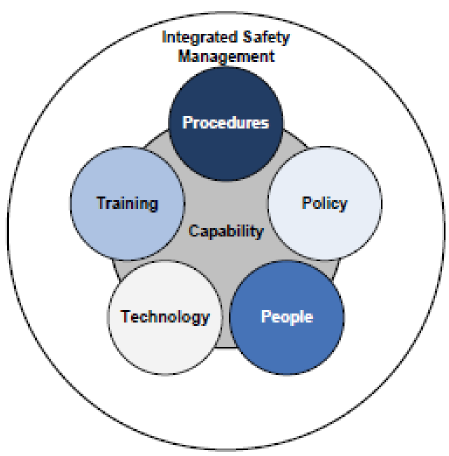


Figure 2.1: Integrated Safety Factors

2.2 Safety Assessment Using the Tenets of SRM and Safety Assurance

In acknowledging the complexity of the NAS and its various system interdependencies, the ATO uses the systematic processes and tenets of SRM and Safety Assurance to identify and address safety hazards and risks across the NAS.

The remainder of this section discusses the foundational concepts and practices used to identify and address safety issues and consider potential ramifications in an integrated way. It will describe at a high level the underlying causes of safety hazards and the means by which the ATO manages and tracks safety risk.

The SRM process provides the framework to track a NAS change after it has been implemented using Safety Assurance functions to determine whether controls and/or safety requirements are performing as intended/designed. Refer to Figure 2.2 for a depiction of the relationship between SRM and Safety Assurance.

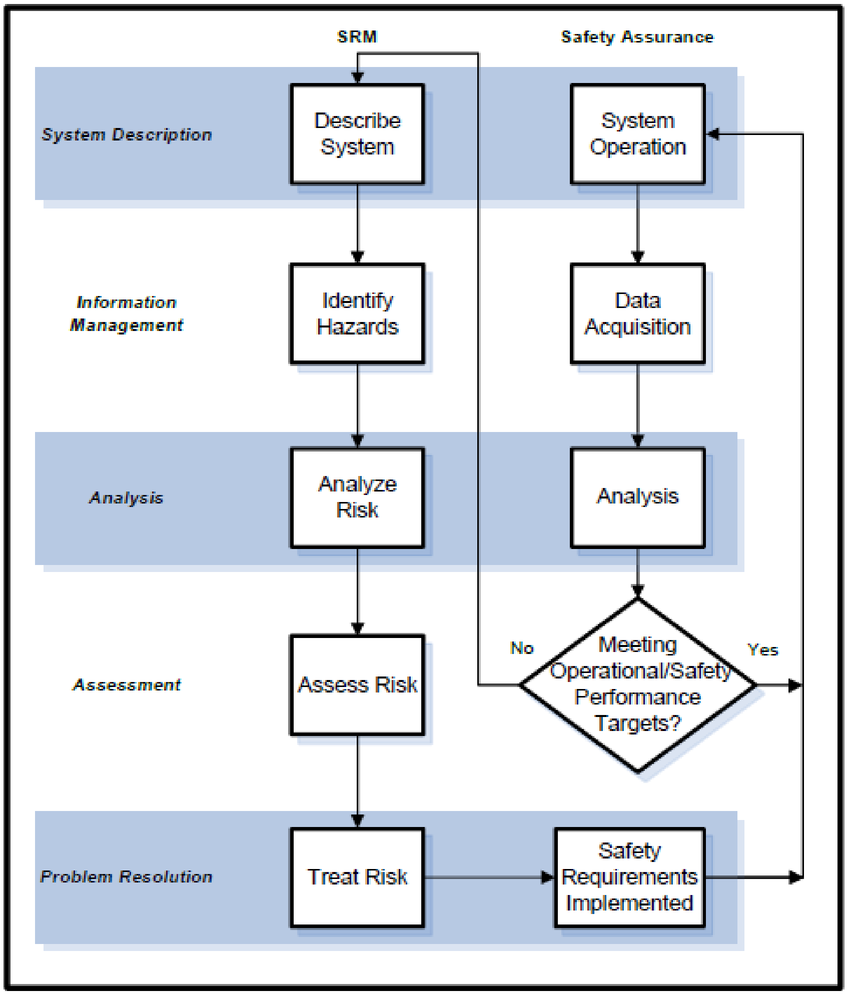


Figure 2.2: SRM / Safety Assurance Process Flow

2.3 SRM: Proactive and Reactive Hazard and Risk Management

SRM is a formalized approach to integrated system safety. It both informs decision-makers about the potential hazards, safety risks, and ways to reduce risk associated with a particular proposal and identifies ways to mitigate existing safety issues in the NAS. The methodology is applied to all NAS equipment, operations, and procedures to identify safety hazards and address risk.

It is necessary to make the approach to managing safety risk into a formalized, objective process. This helps ensure the effective management of a safety hazard's risk. SRM provides a means to:

- Identify potential hazards and analyze and assess safety risk in ATO operations and NAS equipment;
- Define safety requirements to reduce risk to an acceptable level;
- Identify safety performance targets, the measurable goals used to verify the predicted residual risk of a hazard; and
- Create a plan that an organization can use to determine if expected risk levels are met and maintained.

2.4 Safety Assurance: Identifying and Closing Safety Gaps

SRM alone does not ensure the safety of the services the ATO provides; equally important are the efforts performed under the umbrella of Safety Assurance. Safety Assurance builds on SRM efforts by collecting and assessing data to monitor compliance, assess the performance of safety measures, and identify safety trends. It provides the means to determine whether NAS equipment, operations, and procedures—and changes to them—meet or exceed acceptable safety levels. The Safety Assurance component of the Safety Management System (SMS) encompasses all of the ATO processes and programs that survey the NAS. These processes and programs can lead to the discovery of previously unidentified existing safety issues and risk controls that are outdated or no longer effective.

Continuous improvement of the safety of the NAS can occur only when an organization is vigilant in monitoring the performance of its operations and corrective actions. Refer to Section 6 for more information about the ATO programs that fit within the Safety Assurance component of the SMS.

2.4.1 High-Priority Safety Issues

The ATO leverages the vast amount of safety data collected through mandatory, voluntary, and automated reporting programs and stakeholder feedback to identify trending, high-priority safety issues. Further, the ATO develops mitigations and performance targets to address and monitor the safety performance of those issues. The ATO uses SRM principles to guide its process.

When identifying high-priority safety issues in the ATO, observed safety trends are broken down into discrete issues by assessing details such as causal factors and system states. Subject matter experts from stakeholder organizations then participate in the SRM process to perform an in-depth data review and identify mitigations that may reduce the prevalence and/or criticality of the observed safety trend. This team also sets safety performance targets that must be met prior to closing the issue. Safety (AJI) works to ensure mitigations are implemented and monitors each issue against its performance targets to determine when closure of each issue can occur. Mitigations and monitoring strategies are updated on a periodic basis.

2.4.2 Audits and Assessments

To continuously improve the safety of its NAS equipment, provisioned services, operations, and procedures, the ATO conducts audits and assessments to determine whether the NAS is performing as expected. ATO employees also use audit and assessment techniques to test, validate, and verify safety data obtained and produced by the various entities and organizations in the NAS. Furthermore, ATO audits and assessments identify causes and correlations that can improve the understanding of safety performance.

Audits and assessments are defined as follows:

- An assessment is the process of measuring or judging the value or level of something. The objective of an assessment is to determine the organization's ability to achieve its goals and accomplish its mission.
- An audit is a review that verifies conformance to established criteria, processes, and work practices. The objective of an audit is to determine an organization's compliance with FAA directives and procedures.

Audits and assessments verify positive and negative safety trends. If a safety issue or hazard is identified through an audit or assessment, SRM is used to document the hazard and identify mitigations. In this sense, Safety Assurance and SRM complement each other by providing a continuous loop of hazard identification and risk management methods.

Audits and assessments may be scheduled or unscheduled formal reviews; examinations; or verifications of activities, controls, ATO operations, and ATO systems. The scope of safety audit and assessment activities can vary. An audit or assessment can either focus on a single procedure / piece of NAS equipment or broadly examine multiple elements of a system.

The ATO uses both audits and assessments at the facility, district, Service Area, and national levels. Using the above-described methodologies, the ATO assesses safety performance through:

- Proactive evaluation of facilities, equipment, documentation, and procedures (e.g., internal assessments);
- Proactive evaluation of Service Delivery Point performance, thus verifying the fulfillment of Service Delivery Point safety responsibilities (e.g., periodic competency checks in the form of Quality Control, operational skills assessments, and system safety reviews); and
- Periodic evaluations to verify a system's performance in control and management of safety risks (e.g., internal and external audits and assessments).

For additional information about the ATO's audit and assessment program, refer to FAA Order JO 2900.2, *Air Traffic Organization Audits and Assessments.*

2.4.3 ATO Quality Assurance and Quality Control

Requirements and guidance for Quality Assurance and Quality Control are contained in three ATO orders: FAA Order JO 7210.632, *Air Traffic Organization Occurrence Reporting*; FAA Order JO 7210.633, *Air Traffic Organization (ATO) Quality Assurance (QA)*; and FAA Order JO 7210.634, *Air Traffic Organization (ATO) Quality Control*. These orders provide specific direction for the reporting, investigating, and recording of air traffic incidents. Responsibilities for assessing trends and noncompliance are also provided, along with guidance for identifying and correcting performance deficiencies.

2.5 Identifying and Addressing System Vulnerabilities

Before performing SRM, it is important to acknowledge the potential origins of safety hazards in the NAS. Daily operations in an ever-changing air traffic environment can present varying hazards and levels of safety risk. Given the complex interplay of human, material, and environmental factors in ATO operations, the complete elimination of all hazards and safety risk is unachievable. Even in organizations with excellent training programs and a strong safety culture, mechanical and electronic equipment will fail, software will function in an unintended manner, and human operators will make errors.

2.5.1 System Gaps and Hazard Defenses

Developing a safe procedure, hardware, or software system requires that the procedure/system contain multiple defenses, ensuring that no single event or sequence of events results in an incident or accident. Failures in the defensive layers of an operational system can create gaps in defenses, some known and others unknown. Gaps "open" and "close" as the operational situation, environment, or equipment serviceability state changes. A gap may sometimes be the result of a momentary oversight on the part of a controller or operator, typically described as an **active failure**. Other gaps may represent long-standing **latent failures** in the system. Latent conditions exist in the system before negative effects can occur. The consequences of a latent condition may lie dormant for extended periods of time. Figure 2.3 illustrates how an incident or accident can penetrate all of a system's defensive layers.

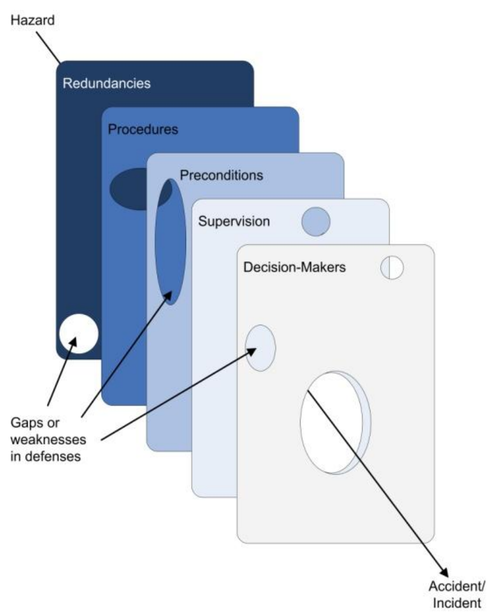


Figure 2.3: Defenses in Depth

These gaps may occur due to:

- Undiscovered and long-standing shortcomings in the defenses,
- The temporary unavailability of some elements of the system due to maintenance action,
- Equipment failure,
- Human interaction, and
- Policy/decision-making.

2.5.2 Hazard Defenses

Designers of NAS hardware and software must strive to design systems that will not impose hazardous conditions during abnormal performance. Using a key systems engineering concept, such systems are referred to as being fault tolerant. A **fault-tolerant** system includes mechanisms that will preemptively recognize a fault or error so that corrective action can be taken before a sequence of events can lead to an accident. A subset of a fault-tolerant system is a system that is designed to be fail safe. A **fail-safe** system is designed such that if it fails, it fails in a way that will cause no harm to other devices or will not present a danger to personnel.

Error tolerance, another systems engineering concept, is a system attribute in which—to the maximum extent possible—systems are designed and implemented in such a way that errors do not result in an incident or accident. An error-tolerant design is the human equivalent of a fault-tolerant design.

Design attributes of an error-tolerant system include:

- Errors are made apparent,
- Errors are trapped to prevent them from affecting the system,
- Errors are detected and warnings/alerts are provided, and
- Systems are able to recover from errors.

For an accident or incident to occur in a well-designed system, gaps must develop in all of the defensive layers of the system at a critical time when defenses should have been capable of detecting the earlier error or failure. Functions, equipment, procedures, and airspace components of the NAS interact through numerous complex relationships. Given the temporal nature of these relationships, the ATO must continuously monitor safety risk to maintain an acceptable level of safety performance and prevent gaps.

2.6 The Human Element's Effect on Safety

Human error is estimated to be a causal factor in the majority of aviation accidents and is directly linked with system safety error and risk. For this reason, hardware and software system designers must eliminate as many errors as possible, minimize the effects of errors that cannot be eliminated, and reduce the negative effect of any remaining potential human errors.

Human performance variability is a limitation that necessitates a careful and complete study of the potential effect of human error. Human capabilities and attributes differ in areas such as:

- Manner and ability of the senses (e.g., seeing, hearing, and touching),
- Cognitive functioning,
- Reaction time,
- Physical size and shape, and
- Physical strength.

Fatigue, illness, and other factors (e.g., stressors in the environment, noise, and task interruption) also affect human performance. Optimally, the system is designed to resist, or to at least tolerate, human error.

When examining adverse events attributed to human error, it is often determined that elements of the human-to-system interface (e.g., display design, controls, training, workload, or manuals and documentation) are flawed. The study of human reliability and the application of human performance knowledge must influence system design for safety systems and be an integral part of risk management. 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 approach is central to the concept of managing human error that affects safety risk.

2.7 Closing Gaps Using SRM and Safety Assurance Principles and Processes

Safety risk can be reduced proactively and reactively. Monitoring operational data, carefully analyzing the system, and reporting safety issues make it possible to proactively detect and prevent sequences of events where system deficiencies (i.e., faults and errors, either separately or in combination) could lead to an incident or accident before it actually occurs. The same approach also can be used to reactively analyze the chain of events that led to an accident or incident. With adequate information, safety professionals can take corrective action to strengthen the system's defenses when devising new air traffic procedures, operations, and NAS equipment or when making changes to them. The following is an illustrative, but not comprehensive, list of typical defenses used in combination to close gaps in defenses:

Equipment defense strategies:

- Redundancy:
  - Full redundancy, which provides the same level of functionality when operating on the alternate system
  - Partial redundancy, which results in some reduction in functionality (e.g., local copy of essential data from a centralized network database)
- Independent checking of design and assumptions
- System design that ensures that critical functionality is maintained in a degraded mode if individual elements fail
- Policy and procedures regarding maintenance to prevent a loss of some functionality in the active system or a loss of redundancy
- Automated aids or diagnostic processes designed to detect system failures or processing errors and to report those failures appropriately
- Scheduled maintenance
- Implementation of robust system development assurance programs in system acquisitions

Operating procedures:

- Adherence to standard phraseology and procedures
- Read-back of critical items in clearances and instructions
- Checklists and habitual actions (e.g., requiring a controller to follow through the projected flight path of an aircraft, looking for conflicts, and receiving immediate coordination from the handing-off sector)
- Inclusion of a validity indicator in designators for Standard Instrument Departures and Standard Terminal Arrival Routes
- Training and reporting methods

Organizational factors:

- Management commitment to safety
- A strong, positive safety culture
- Safety policy implementation with adequate funding provided for safety management activities
- Oversight to ensure that correct procedures are followed
- A zero-tolerance policy toward willful violations or shortcuts
- Control over the activities of contractors

2.8 Safety Order of Precedence

The methods for reducing safety risk generally fall under one of the four categories that make up the Safety Order of Precedence. The Safety Order of Precedence categorizes safety risk mitigations in the following order of preference:

Table 2.1: Safety Order of Precedence and Examples

Priority	Definition	Example
1.	**Design for minimum risk** - Design the system (e.g., operation, procedure, human-to-system interface, or NAS equipment) to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level by selecting alternatives.	During airport planning, avoid intersecting runways if possible.
2.	**Incorporate safety devices** - 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 function checks.	Install an Engineered Materials Arresting System, which uses crushable material placed at the end of a runway to stop an aircraft that overruns the runway.
3.	**Provide warning** - When alternatives and safety devices do not effectively eliminate or reduce risks, use warning devices or procedures to detect the condition and produce an adequate warning. The warning is designed to minimize the likelihood of inappropriate human reaction and response and must be provided in time to avert the hazard's effects.	Install a lighting system to alert pilots/controllers of potential unauthorized crossings. Provide new runway or taxiway markings.
4.	**Develop procedures and training** - When it is impractical to eliminate risks through alternative selection, safety features, and warning devices, use procedures and training. However, management must concur when procedures and training alone are applied to reduce risks of catastrophic or hazardous severity.	Develop new taxi and departure/arrival procedures for intersecting runway operations. Train pilots and controllers on new procedures for intersecting runways.

Note: Reliance solely on training is normally not a sufficient means to mitigate safety risk.

3.1 Scope of the Safety Risk Management Process

The Air Traffic Organization (ATO) Safety Risk Management (SRM) process is used to determine the safety risk of National Airspace System (NAS) changes or existing safety issues associated with the provision of air traffic management services. These services include the acquisition, operation, and maintenance of hardware and software; management of airspace and airport facilities; and development of operations and procedures. Security (e.g., physical, information, and cyber), environmental, or occupational safety and health issues that potentially affect the provision of air traffic management services should be considered during the SRM process. Conversely, if these issues do not have an effect on the safe provision of air traffic management services, these issues should not be considered.

It is important to note that the SRM process is not designed to and should not be used to account for programmatic considerations that are related to the environment, finance, budget, or labor/human resources. Additionally, safety hazards associated with the environment, occupational safety, or security that can or do affect the provision of air traffic management services must be reported to the appropriate authority.

This section provides a linear SRM process to follow, guidelines to identify safety hazards and mitigate their risks, and requirements for the development of consistent and thorough safety analyses. Using the steps in this section to perform SRM will not always result in an exhaustive study of air traffic procedures, operations, or NAS equipment (i.e., hardware and software). The appropriate level of detail used when conducting SRM depends on the complexity, size, and potential effect of the NAS change or existing safety issue. Figure 3.1 provides a high-level depiction of the key steps, decision points, and outputs of the SRM process.

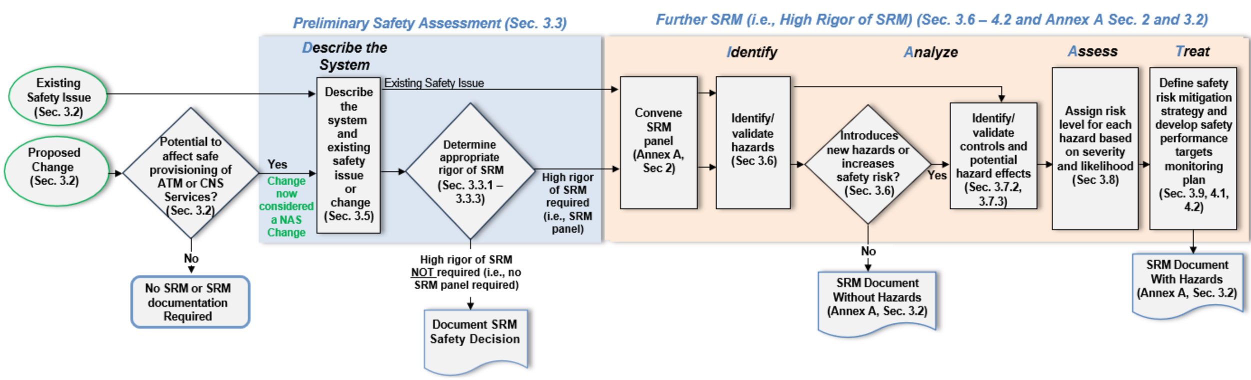


Figure 3.1: SRM Process

3.2 Triggers for SRM and Identifying NAS Changes

SRM is performed to analyze and address an existing safety issue or when a NAS change is proposed. **An existing safety issue** is a contributing factor or finding in the current NAS that has led to, or could lead to, an unsafe outcome. Requests for action to address such issues may be proposed and initiated as part of a Safety Assurance function. This is usually a result of Quality Assurance, audits, or assessments. If a request to take action on an existing safety issue is received, SRM must be performed. More information and considerations regarding existing safety issues are contained in Section 3.5.6.2.

All proposed changes to the NAS require the change proponent to determine whether the change is a NAS change. A **NAS change** is a modification to any element of the NAS that pertains to, or could affect, the safe provision of Air Traffic Management (ATM) and/or

Communication, Navigation, and Surveillance (CNS) services (ATM/CNS). For example, air traffic controllers and Technical Operations specialists, their training, and their certification are elements of the NAS and directly relate to the safe provision of air traffic services. Such changes encompass a wide range of updates and modifications to local and national air traffic procedures and processes, airspace configurations, equipment/systems, maintenance protocols, and related operating standards and requirements that support the safety, efficiency, and adaptability of the NAS. Sections 3.3, 3.3.1, and 3.3.2 provide guidance on how to continue/complete the Preliminary Safety Assessment for NAS changes and determine the appropriate rigor of the SRM effort.

Changes that **do not** impact the safety of ATM or CNS services **are not** NAS changes, and they do not require SRM or any SRM documentation. However, in cases of uncertainty in determining whether a proposed change is a NAS change, the change proponent may choose to complete the "Describe the System" phase of the **DIAAT process** and/or document the determinations in an SRM Safety Decision. (See Section 3.4 for a description of the DIAAT process, Section 3.5 for information on the "Describe the System" DIAAT phase, and Annex A, Section 3.2, for SRM Safety Decision documentation conventions.) The list below, though not exhaustive, provides examples of changes that are **unlikely to be NAS changes and do not require SRM or SRM documentation**:

- Editorial or administrative changes to documentation, guidance, or directives.
- Modifications made to systems to meet initial operational specifications or meet baseline configuration in NAS-MD-001 if the system specifications have previously undergone SRM. The modification and testing processes must also be compliant with the Safety Management System (SMS).
- Facility layout/redline/end-state drawings (e.g., Air Route Surveillance Radar (ARSR), Airport Traffic Control Tower (ATCT), Terminal Radar Approach Control Facility, or Air Route Traffic Control Center (ARTCC)), as identified in the Configuration Control Board Charter, Appendix A.
- Installation or moving of equipment if such activities do not deviate from defined installation siting processes.

3.3 The Preliminary Safety Assessment: Describing the System to Identify SRM Requirements

The primary objective of conducting SRM for a proposed change is to determine whether the change could negatively affect safety risk in the NAS (i.e., introduce hazards or increase the risk associated with existing hazards). After the change proponent determines the change **is** a NAS change (i.e., a change with the potential to affect the safe provision of ATM/CNS services), the change proponent must complete the "Describe the System" phase of the DIAAT process to provide a description of the change and the system in which it will occur. (See Section 3.4 for a description of the DIAAT process, and Section 3.5 for information on the "Describe the System" DIAAT phase.) The description of the system must address system boundaries, system interfaces and interactions, affected stakeholders, and temporal impacts of the change on the current system. The change proponent documents these findings in an SRM Safety Decision or (if an SRM panel convenes) an SRM document and uploads the documentation, after completion of the required SRM activities, in the Safety Management Tracking System (SMTS).

In addition to identifying whether a change is a NAS change, the change proponent must consider a NAS change's scope and complexity to ensure the rigor of the SRM effort (i.e., the depth and detail of the safety analysis) is commensurate with the NAS change's potential impact on the provision of ATM/CNS services. This requires the change proponent to consider whether the NAS change has the potential to introduce hazards or increase safety risk by conducting a simple analysis of the system and change description. Depending on the scope of the change, this can be difficult if the change or the system in which it will occur interfaces or interacts with other NAS systems. This is a likely factor as systems in the NAS continue to evolve. The change proponent may use the information in Sections 3.3.1 through 3.3.3 to complete/continue the Preliminary Safety Assessment and determine the appropriate rigor of the SRM effort. Additionally, change proponents are encouraged to use the information in Section 3.5.2 to address potential gaps created by the NAS change within the current system and to contact their Service Center or a Safety (AJI) **Safety Case Lead (SCL)** if they need additional guidance.

NAS changes with no potential to introduce hazards or increase safety risk may only require a description of the change and the system in which it will occur (i.e., documentation of the system and change description), simple consideration of potential to introduce hazards / increase safety risk, and documentation of the rationale for why the NAS change has no potential to affect safety in the provision of ATM/CNS services. These items must be recorded in an SRM Safety Decision and uploaded in SMTS. (See Annex A, Section 3.2, for documentation requirements.) In contrast, more complex NAS changes—those with higher potential to affect safety risk in the provision of ATM/CNS services—require high rigor of SRM. Thus, the change proponent must complete subsequent phases of the DIAAT process, usually through an SRM panel. (Special considerations apply for certain local NAS changes. See Section 3.3.3 for more information.)

3.3.1 Defining Appropriate Rigor of SRM for NAS Changes: Continuing the Preliminary Safety Assessment

Defining the appropriate rigor of an SRM effort (i.e., the depth and detail of the safety analysis) entails determining which phases of the DIAAT process are required for analyzing the NAS change's potential to affect safety risk in the provision of ATM/CNS services. Determining the appropriate rigor is increasingly difficult as system interfaces and interactions in the current NAS become more complex and evolve. The information in Section 3.5.2 is helpful for considering issues surrounding system interfaces and interactions within the current system, and SRM experts in the Service Centers and AJI SCLs are good resources for ensuring satisfaction of SRM requirements.

To determine the required rigor of the SRM effort, the change proponent first considers whether the NAS change is compliant with current FAA policies and aligns with (and does not deviate from) processes that have previously undergone SRM and have been documented and approved by the appropriate management officials. If the NAS change meets these conditions and there are no safety concerns with implementing the NAS change, the change proponent will have fulfilled SRM requirements with the completion of the "Describe the System" phase of the DIAAT process and consideration of whether the NAS change has the potential to introduce hazards / increase safety risk. The change proponent must simply document this information and their findings in an SRM Safety Decision with information supporting why there are no safety concerns. (See Annex A, Section 3.2, for SRM Safety Decision documentation requirements.) Similarly, many routine, repeatable NAS changes occur in accordance with FAA and/or ATO documents, and they comply or align with current FAA policies and processes. Such changes may include, for example, changes to field-level policies, directives, manuals, Standard Operating Procedures (SOPs), Letters of Agreement (LOAs), and Letters of Procedure (LOPs). If such changes do not deviate from existing organizational standards, requirements, and protocols, they may not require high rigor of SRM (i.e., analysis of the NAS change through an SRM panel) to fulfill SRM requirements. However, policy compliance and conformity with established operating practices are not the only factors to consider when determining the necessary rigor of SRM for a NAS change. Thus, further assessment is required.

Continuing the Preliminary Safety Assessment, the change proponent must evaluate all potential sources of safety risk to ensure a NAS change will not introduce hazards or increase safety risk. Unanticipated safety events often occur during the transition to the new way of operating or when introducing a new procedure or process that is unfamiliar to its users. This is especially true for changes that differ substantially from current operating practices or conditions. Such changes require change proponents to assess possible impacts on procedures and processes that interact with the NAS change (including NAS equipment and systems), as well as the effects of the change's modifications to current operations and the system state in which the modifications will occur. Additionally, the change proponent must evaluate the plans for implementing the change to ensure that typical implementation safety concerns are addressed; any routinely applied, safety-related implementation measures are executed; and follow-up activities (e.g., monitoring) confirm expected safety outcomes. (Note: It is difficult for national SRM efforts to consider all facility-specific sources of risk / potential hazards (i.e., those related to the unique local environment, or facility-level waivers to FAA orders and directives). Local SRM should consider all potential effects on facility air traffic management and associated equipment and systems when implementing a nationally developed change.) NAS changes for which the change proponent identifies no potential sources of hazards or increased safety risk and that do not deviate from existing organizational standards, requirements, and protocols commonly do not require any further SRM. However, the change proponent must document the findings from the completed "Describe the System" phase of the DIAAT (i.e., the description of the NAS change and the system in which it will occur) in an SRM Safety Decision with their reasoning for why the NAS change has no potential to introduce hazards or increase safety risk. (See Annex A, Section 3.2, for documentation requirements.)

For some NAS changes—those with higher potential to affect safety risk in the provision of ATM/CNS services—identification of all potential sources of risk requires more than the change proponent's simple consideration of potential hazards / increases in safety risk. Such cases would require formal completion and documentation of at least one additional phase of the DIAAT process (if it is a local NAS change) **or** would require high rigor of SRM—the completion of further SRM via an SRM panel. (Considerations for local NAS changes are described in Section 3.3.3.) Change proponents should use all available resources to support making an informed decision regarding the appropriate rigor of SRM to ensure the depth and detail of the SRM effort is commensurate with the NAS change's potential to impact safety risk in the NAS. This may involve consulting SRM or technical experts from relevant agency offices or coordinating with affected stakeholders (e.g., local personnel) to identify potential safety impacts. Leveraging input from these individuals can assist change proponents in determining if it is necessary to convene an SRM panel.

Section 3.3.2 provides examples of NAS changes and their appropriate levels of rigor for SRM. If there is uncertainty about the safety implications of a NAS change or the appropriate rigor of SRM efforts, contact the appropriate Service Center Safety Office (for local changes) or an AJI

SCL via the ATO SMS mailbox for assistance.[1] (See the AJI SRM Pre-Panel webpage for Service Center contact information.)

3.3.2 Examples of NAS Changes and Their Appropriate Rigor of SRM

This section provides guidance on the appropriate rigor of SRM for national and local NAS changes according to the changes' ability to affect safety risk in the NAS. Service Center SRM specialists and/or AJI SCLs can provide further guidance or assistance in determining the appropriate level of rigor for a specific NAS change.

The list below, though not exhaustive, presents examples NAS changes that commonly do not require high rigor of SRM (i.e., completion of all DIAAT process phases with an SRM panel). Changes that do not require high rigor of SRM may only require completion of the "Describe the System" phase of the DIAAT process (described in Section 3.5), the change proponent's simple consideration of the NAS change's potential to introduce hazards / increase safety risk, documentation in the SRM Safety Decision, and entry of the SRM Safety Decision in the SMTS. See Annex A, Section 3.2, for documentation requirements of a complete SRM Safety Decision.

i. NAS Changes that Commonly Do Not Require High Rigor of SRM:

- Nationally developed changes to local (facility-level) Air Traffic Control (ATC) procedures to comply with FAA or ATO safety guidance, or to accommodate implementation of new NAS-wide equipment or systems when nationally developed guidance is provided for use at the local level. The facility must not deviate from the FAA or ATO safety guidance or Program Office requirements for modifying local-level procedures.

  Note: If deviations or additional changes are made in these procedures, or if the national guidance does not address all local-level concerns with implementation of the change, subsequent DIAAT phases are required to fulfill SRM requirements. See Section 3.3.3 for special considerations for local NAS changes or see Annex A for guidance on convening an SRM panel.

- Changes to local (facility-level) ATC procedures and practices, typically defined in an LOA, LOP, or SOP, that do not deviate from existing FAA/ATO policies and processes and do not have any anticipated safety concerns associated with implementation (e.g., completing required training/briefings, coordination, outreach, and ensuring proficiency in application of the changes).
- Routine, standard closures of runways and taxiways (or ramps) for maintenance or minor surface/equipment/system modifications as long as:
  - They are associated with Airport and ATC operating procedures that do not deviate from existing FAA/ATO policies and processes,
  - They have not previously resulted in safety events and/or are not associated with known NAS safety issues or trends, and
  - They occur for short periods of time and have Airport and/or ATC procedures and responsibilities defined in a local LOA or SOP.

1. AJI SCLs are experts in SMS policy and guidance that pertain to the ATO. Refer to the SRMGSA for a description of their roles and responsibilities.

Some local changes or local implementation of NAS changes may require the change proponent to convene an SRM panel; however, special considerations may apply. (See Section 3.3.3 for more information.)

List ii below describes NAS changes that typically require higher rigor of SRM efforts. (This is not an exhaustive list.)

ii. NAS Changes that Commonly Require High Rigor of SRM:

- Operational/procedural changes or waivers that are not defined in an existing order (e.g., flight trials, tests, demonstrations, and prototypes that are live in the NAS).
- Any waiver or change to an order if the order implements a new procedure that, when followed, could affect the safe provision of air traffic services.
- Introduction of navigation procedures into the NAS.
- Changes to separation standards.
- Airport building construction; addition of, modification to, prolonged closure of, or removal of an airport, runway, or taxiway; and changes to airport/runway/taxiway lighting.

  Note: Many of these changes are proposed and sponsored by the Office of Airports (ARP). ARP SMS requirements are documented in FAA Order 5200.11, *FAA Airports (ARP) Safety Management System*. The ATO must maintain awareness of airport construction projects to ensure ATO SRM (separate from ARP SRM efforts) is performed when construction projects could affect ATM/CNS services.

- New NAS systems used in ATC or pilot navigation—or new uses for such existing systems—regardless of their applicability to the FAA Acquisition Management System (AMS).
- System Support Directives that introduce new and/or changed requirements, functionalities, or capabilities for operational systems/equipment in the NAS, such as:
  - Communication, navigation, and surveillance systems
  - Weather products/services
  - Displays
  - Alerting and advisory systems
  - Service provider equipment (e.g., the Automatic Dependent Surveillance–Broadcast (ADS-B) system and FAA Telecommunications Infrastructure)
  - Decision support tools
- Modifications that do not meet the acquisition design assurance level requirement
- Changes to Maintenance Technical Handbooks or Technical Instruction Books to include changes to:
  - Methods or techniques for existing maintenance tasks
  - Periodicity of existing periodic maintenance

- Standards or tolerances
- Adding new maintenance procedures
- Removing maintenance procedures
- Changes to certification
- Adding or removing electronic Technical Performance Record (eTPR) requirements

- Removal, discontinuation, deactivation, or decommissioning of NAS equipment, procedures, systems, or services
- Site adaptations if the technical limits of the adaptations are deviations from the baseline configuration as defined in NAS-MD-001, or out-of-system specification conditions
- Local adaptations (e.g., resulting from a Program Trouble Report)
- ATC facility changes, including:
  - Tower siting or relocation
  - Facility relocation
  - Cab replacement or redesign
  - Permanent consolidation or de-consolidation of facilities
  - Facility split
  - Temporary tower use or introduction
- All charting specification changes prior to submission to the Interagency Air Committee for final signature (e.g., symbology, color changes in routes, and route identifiers)
- Airspace changes, including routes, airways, and sectors, and the addition or deletion of a position or sector
- Removal of, or modifications/waivers to, existing national and/or local training requirements that could affect the NAS or NAS operations, except when they are related to Individual Performance Management
- Establishment of or modifications to technical training orders, architecture, and curricula (Note: This excludes training for Airway Transportation Systems Specialists.)
- Emergency modifications in the NAS (see Section 3.6.3.3 for more information)

3.3.3 Special Considerations for Local NAS Changes

When a NAS change involves multiple stakeholders, cross-organizational expertise, or significant safety implications, convening an SRM panel ensures that the SRM effort includes the appropriate level of detail. However, many NAS changes occur at the local (e.g., facility) level, where the change may be less complex and have fewer potential effects on system safety. Although they still require SRM, these changes may not require a high rigor of SRM (i.e., convening an SRM panel) to fulfill SRM requirements. When specific criteria are met, the change proponent can choose to conduct a **Two-Phase Local SRM** process, which involves completing the “Describe the System” and “Identify Hazards” phases of the DIAAT process with input from stakeholders of the change. (See Section 3.5 and Section 3.6 for descriptions of these DIAAT phases.) These two DIAAT phases help determine whether a local-level NAS change has the potential to introduce hazards or increase safety risk. Should no hazard be identified through this two-phase process, the change proponent must document the findings in a SRM Safety Decision—including a rationale for a safety finding without hazards—and upload it in SMTS. (See Annex A, Section 3.2, for documentation requirements.) However, if completion of this two-phase process uncovers the potential for the proposed change to introduce hazards or increase safety risk, the change proponent must convene an SRM panel and conduct subsequent phases of the DIAAT process.

3.3.3.1 Differences Between a Two-Phase Local Process and an SRM Panel

While assembling experts to review a system and identify hazards is a core component of both Two-Phase Local SRM and formal SRM panels, the two processes differ significantly in their execution, authority, and documentation requirements. Change proponents must understand these distinctions to ensure the SRM process is consistently and appropriately applied. The list below identifies ways in which the Two-Phase Local SRM process and an SRM panel differ:

- **Facilitation:** In Two-Phase Local SRM, the meeting can be facilitated by the change proponent or a designated member of the group, provided they have appropriate ATO SMS and SRM training (e.g., SRM Practitioner training). Additionally, the Two-Phase Local SRM process may be facilitated through any means of correspondence that allows input from stakeholders, including non-linear forms of virtual communication (e.g., email). An SRM panel requires that a facilitator possess a higher level of SRM expertise to lead the consensus-driven risk analysis, assessment, and treatment discussions; and an SRM panel conducts its analysis in real time with stakeholders present in person or through linear forms of virtual communication (e.g., online conference).
- **Process Objectives and Limitations:** Two-Phase Local SRM is an initial, preliminary assessment limited to conducting only the "Describe the System" and "Identify Hazards" phases of the DIAAT process. An SRM panel, however, may additionally involve risk analysis, assessment, and treatment, and development of a monitoring plan.
- **Participation:** Two-Phase Local SRM relies on a small, localized group of technical experts and stakeholders, including facility bargaining unit representatives. An SRM panel involves a more rigorous roster of participants with strictly separated roles, including SRM panel members who make consensus-driven safety risk determinations, Subject Matter Experts (SMEs) from a broader range of FAA offices and non-governmental organizations, and observers such as district-level Air Traffic Services (AJT) leadership and the Air Traffic Safety Oversight Service (AOV).
- **Documentation:** The outcome of a Two-Phase Local SRM process that finds no hazards is documented in an **SRM Safety Decision**, which is a shorter-form document than an SRM Document With / Without Hazards. The latter document, completed by an SRM panel, may contain sections for detailing the risk analysis, assessment, and treatment, and a Monitoring Plan.
- **Signatures Requirements:** An SRM Safety Decision for Two-Phase Local SRM always requires an approval signature from a Manager at the district or equivalent level (or above) to attest to their awareness of the SRM activity, along with a concurrence signature regarding the SRM process. SRM Documents With and Without Hazards for SRM panels may require similar Approval and Risk Acceptance signatures, but the requirements vary by risk level and may require additional signatures from organizations outside the ATO.
- **Potential Process Outcomes:** The Two-Phase Local SRM process is designed specifically to identify when a higher rigor of SRM is needed. When no potential for

hazards is identified during this process, the requirement is to simply document the SRM Safety Decision with a rationale for the safety finding without hazards. However, if **any** stakeholder involved in the Two-Phase Local SRM activity identifies a potential for the NAS change to introduce hazards or increase safety risk, the change proponent must initiate actions to convene a full SRM panel.

3.3.3.2 Criteria for Applying a Two-Phase Local SRM Process

The Two-Phase Local SRM process can be used when the change meets **all** of the following criteria:

i. The change is "local" as defined in Section 5.2.

ii. The change is consistent with established organizational policies and processes and/or a standard, routinely used operating practice in NAS facilities.

iii. The change proponent is not aware of any national or local safety events or trends or local safety issues similar to or associated with the proposed change.

iv. The SRM effort is not addressing an existing safety issue formally identified via ATO/FAA QC/QA processes (see Section 3.5.6.2) or an Obstruction Evaluations Group (OEG) aeronautical study analysis determination.

v. The change does not involve sector/position modifications or an airspace modernization project, facility realignment, or airspace redesign effort (e.g., lateral sector boundary and/or altitude stratum modifications), as referenced in FAA Order JO 7210.67, *Policies and Procedures for Validating New/Revised Sectors/Positions in En Route and Terminal Air Traffic Facilities*.

vi. The change does not involve Department of Defense ATC procedures, Special Use Airspace (SUA), or operations with foreign service providers (i.e., outside the limits of FAA jurisdiction).

vii. The change does not involve ATC facility changes (see Section 3.3.2) or new/modified facility infrastructure, equipment, or systems; non-FAA equipment or systems; or emergency modifications (see Section 3.6.3.3).

viii. The change does not require a waiver per Appendix A, Section 2.2.

If a proposed change meets all the above criteria, the change proponent may choose to apply the Two-Phase Local SRM process (in lieu of conducting an SRM panel) for any of the reasons listed below. (This is not an exhaustive list.)

- It is difficult for the change proponent to determine the appropriate rigor of SRM because the change does not clearly align with the examples provided in Section 3.3.2.
- The change proponent thinks the local NAS change may not introduce hazards /increase safety risk, but there is potential for unknown safety impacts during or after implementation.
- The NAS change in question is a nationally developed change that requires local SRM, and expectations for local modifications/adaptations—such as site-specific procedural adjustments—have been provided (for example) via safety requirements or ATO guidance; but the national guidance does not address all components of the change. In this case, the change proponent must ensure the appropriate rigor of SRM for any

locally developed additions to the change. (Note: This does not apply where a waiver is required.)

3.3.3.3 Conducting the Two-Phase Local SRM Process

To conduct a Two-Phase Local SRM process, the change proponent confirms the change meets the criteria in Section 3.3.3.1, then completes the following steps:

1. Complete the "Describe the System" phase of the DIAAT, providing a detailed description of the current system and the proposed change to support hazard identification discussions. (This phase of the DIAAT process is described in Section 3.5.)
   Note*:* The description of the current system must include all elements of the 5M model. See Section 3.5.6.3 for more information.
2. Assemble an appropriate group of technical experts. This group should include:
   a. An individual with the appropriate ATO SMS and SRM training[2] to support the group in applying hazard identification concepts to identify potential hazards (see Section 3.6). The change proponent or a designated member of the group may fulfil this role.
   b. Stakeholders, SMEs, and representatives of other facilities/entities/programs, etc., that may be affected by the change.
   c. Bargaining Unit representatives (adhere to the Collective Bargaining Agreement between the FAA and the affected bargaining unit).
3. With the group of experts, review the system and change details, and complete the "Identify Hazards" phase of the DIAAT process. (This phase of the DIAAT process is described in Section 3.6.) This entails performing a preliminary hazard analysis to identify any potential to introduce hazards or increase safety risk. This process can occur through an in-person, virtual, or hybrid meeting, or any established communications method that allows the process to be correctly completed and documented.
4. Follow the steps below that are appropriate for the outcomes of the Two-Phase Local SRM analysis:
   a. If no members of the group identify a potential to introduce hazards or increase safety risk:
      - Record this determination and the group's rationale in the SRM Safety Decision. (See Annex A for documentation requirements.)
      - Upload the completed SRM Safety Decision to SMTS.

[2]. FAA Order JO 1000.37C, Appendix A, identifies the training required for all ATO employees and contractors tasked to perform ATO SRM functions.

b. If any member of the group identifies a potential to introduce hazards or increase safety risk:

- Record these results in the SRM Safety Decision. (See Annex A for documentation requirements.)
- Upload the completed SRM Safety Decision to SMTS.
- Initiate actions to convene an SRM panel.

Contact the appropriate Service Area Quality Control Group for SRM guidance and/or support, including assistance with the Two-Phase Local SRM process. (See the AJI SRM Pre-Panel webpage for contact information.)

3.3.4 Considerations for NAS Change Proposals

The configuration management requirements from the NAS Change Proposal (NCP) process may not specifically relate to safety effects. When a NAS change covered by an NCP requires SRM, the appropriate documentation must be included in the material provided to the Configuration Control Board. In terms of SRM, an NCP can be categorized as one of the following:

- Does not require SRM
- Requires SRM (refer to Annex A)

For more information on NCPs, refer to FAA Order 1800.66*, Configuration Management Policy*.

For information on SRM for technology refreshment portfolios, see the Safety Risk Management Guidance for System Acquisitions (SRMGSA).

3.4 SRM Process Phases

SRM is conducted through the DIAAT process, in which there are five potential phases (presented in Figure 3.2). The DIAAT phases are described in detail in Section 3.5 through Section 3.9.

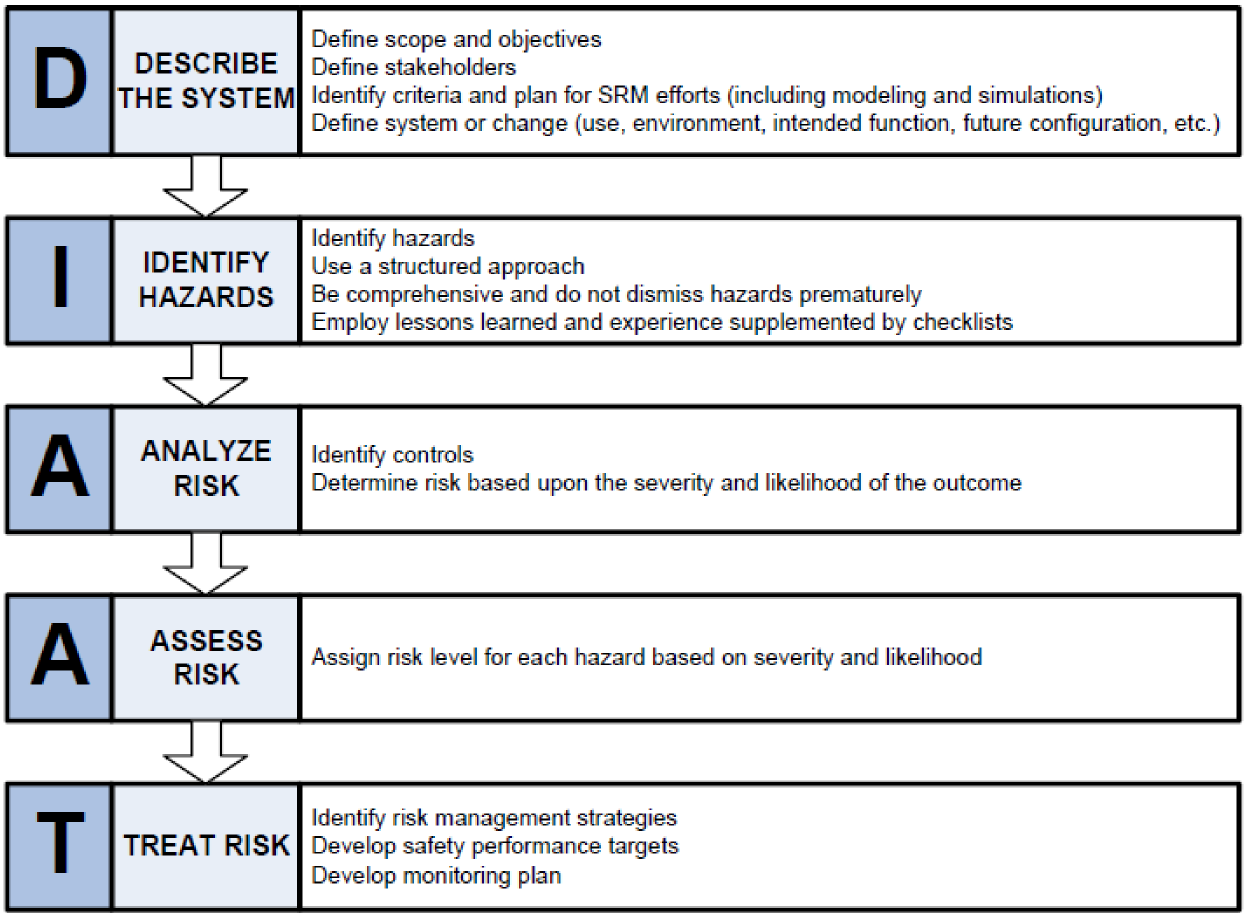
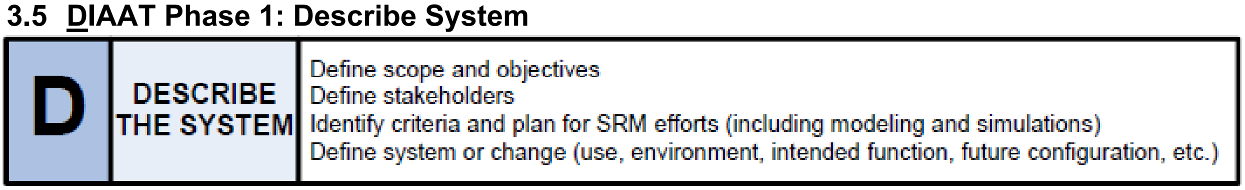


Figure 3.2: DIAAT Process

3.5 DIAAT Phase 1: Describe System



3.5.1 Overview

As discussed in Section 3.2, NAS changes may be proposed and initiated as part of implementation plans for new or modified air traffic procedures, operations, or NAS equipment, or in response to existing safety issues in the NAS. As part of any pre-SRM panel activities and any follow-on SRM panel activities, it is important to develop a detailed description of the NAS change and/or current system and its affected elements.

Note: SRM for mitigations to existing hazards that were identified through safety audits or post-event safety risk analyses should use the event or situation that led to the realization of the hazard's effect(s) as the basis for the documented system description. Use this section as guidance, but refer to Section 3.6.3 for further information.

3.5.2 Bounding SRM in an Integrated NAS

Bounding refers to the process of limiting the analysis and assessment of a change or system to only the elements that affect or interact with each other to accomplish the central function of that change or system. In many cases, there may be a limited or incomplete understanding of the air traffic environment in which the NAS equipment, operation, or procedure will be employed, or the interconnected systems with which the changing system must be integrated for effective operation. Furthermore, the scope for other associated NAS equipment, operations, or procedures may be unknown. Thus, it becomes difficult to ensure that there are no gaps across the boundaries of the change or system. As a result, the scope may be inadvertently set at an inappropriate level.

In light of these potential difficulties, the scope must be set such that gaps are eliminated. As systems become increasingly more complex, interactive, and interrelated, the analysis and assessment of potential safety risk must be integrated temporally, by domain, and across locations. Figure 3.3 provides a visual representation of this integration. Where time is concerned, it is important to consider whether potential safety risk mitigations implemented in the short term will be adequate years into the future when other systems are introduced in the NAS, or whether other follow-on mitigations will negate the effect of those implemented in the past.

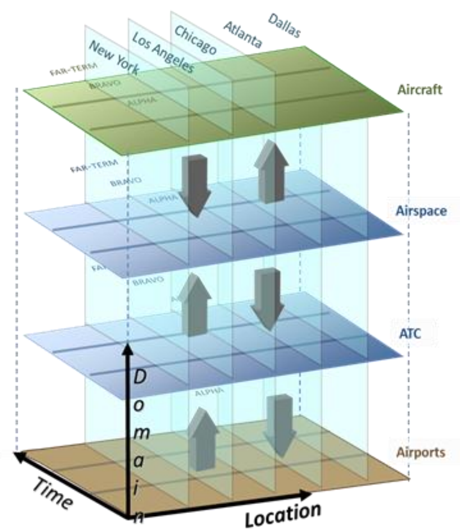


Figure 3.3: The Complex Integration Aspects of a Capability

Figure 3.4 depicts the potential scope and level of SRM required based on the potential impact and scope of the NAS change. The lowest-tiered SRM focuses on identifying hazards associated with individual projects/programs and individual changes to the NAS that are often associated with new system acquisitions. The middle tier is the capability level. Examples of capabilities include Performance Based Navigation, Surface Operations, or Data Communications. Here, system safety risk analyses and assessments become more complex, considering multiple combinations of dependent functions. The top tier represents high-level SRM activities associated with service levels and/or domains to reflect a strategic view of safety across the NAS. Safety management at this level is more static in nature (i.e., essentially non-recurring system safety engineering). It employs high-level functional hazard analyses to identify NAS-level hazards and safety requirements that flow down vertically to the other-tiered levels.

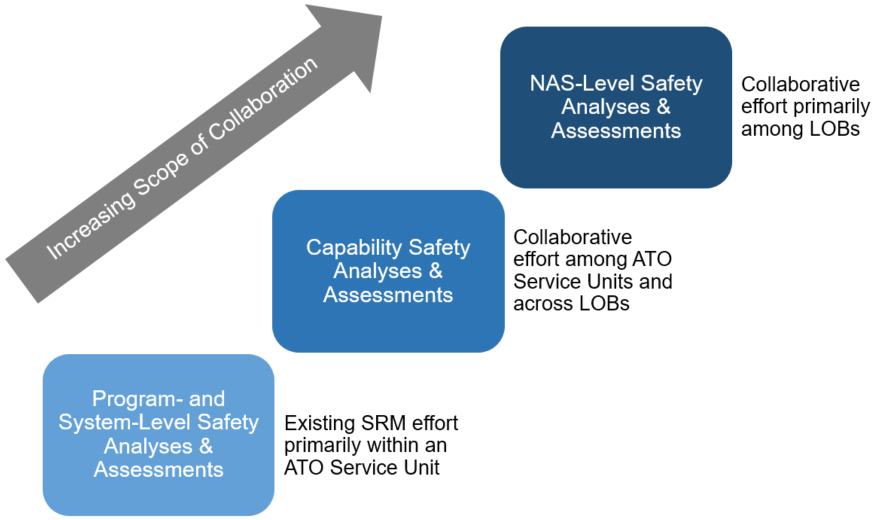


Figure 3.4: Three Tiers of Integrated Safety Management

3.5.3 Depth and Breadth of the NAS Change or Existing Safety Issue

In general, SRM for more complex and far-reaching NAS changes or existing safety issues will require a greater scope and more detail. When evaluating a NAS change or existing safety issue, consider any potential effects on organizations outside the ATO (e.g., Aviation Safety and ARP). Consider the following factors:

- **The depth of the NAS change or existing safety issue.** The complexity and nature (i.e., operational or system acquisition) of the NAS change will dictate the type and number of analyses or assessments required.
- **The breadth of the NAS change or existing safety issue.** The scope of SRM will require additional details when the NAS change affects more than one organization or Line of Business (LOB).

3.5.4 Involving Other FAA LOBs

When ATO SRM impacts FAA LOBs and/or organizations outside the ATO, the provisions and guidance in FAA Order 8040.4, *Safety Risk Management Policy*, apply. Refer to Section 3.6.7 for information on coordinating and addressing safety issues. Refer to Section 5.4.1 and Section 5.4.2 for discussion on cross-LOB risk acceptance.

3.5.5 Setting the Scope of Individual SRM Analyses and Assessments

Guidelines to help determine the scope of individual SRM analyses and assessments include:

- Having a sufficient understanding of system boundaries, including interfaces with peer systems, larger systems of which the system is a component, and users and maintainers;
- Determining the system elements that interact or sub-system components that may be affected; and

- Limiting the system to those elements that affect or interact with each other to accomplish the mission or function.

When setting the scope of individual SRM analyses and assessments:

- Define the relationships/interactions of the NAS change.
- Identify temporal aspects of these relationships/interactions.
- Collect safety documentation that has determined the building blocks of the NAS change.
- Set the scope wide enough to determine the aggregated risk and address any gaps.

3.5.6 Describing the System / NAS Change

System descriptions need to exhibit two essential characteristics: correctness and completeness. Correctness means that the description accurately reflects the system without ambiguity or error. Completeness means that nothing has been omitted and that everything stated is essential and appropriate.

The system description provides information that serves as the basis for identifying all hazards and associated safety risks. The system/operation must be described and modeled in sufficient detail to proceed to the hazard identification stage of the DIAAT process. For example, modeling might entail creating a functional flow diagram to help depict the system and its interface with the users, other systems, or sub-systems.

As discussed, the system is always a component of some larger system. For example, even if the change encompasses all services provided within an entire ARTCC, that ARTCC can be considered a subset of a larger body of airspace, which in turn is a subset of the NAS.

3.5.6.1 Considerations for NAS Changes

Complex NAS changes may require a detailed system description that includes numerous charts, drawings, design descriptions, and/or narratives. Simple NAS changes may only require one or two paragraphs describing the system and NAS change. The description must be clear and complete before continuing the SRM process. Questions to consider include:

- What is the purpose of the NAS change?
- What issue is necessitating the NAS change?
- How will the change be used / function in the NAS?
- What are the boundaries and external interfaces of the NAS change or system?
- In what environment will the system or NAS change operate?
- How is the system or NAS change interconnected/interdependent with other systems?
- How will the NAS change affect system users/maintainers?
- If the NAS change is a waiver/renewal, how could other waivers in effect interact with it?

The following are examples of information to consider when describing the system:

- Average annual approaches to each runway
- Fleet mix
- Number and type of airport operations

- Number of aircraft controlled (ground, pattern, and transitions)
- Number of hours the airport operates and number of aircraft controlled under Visual Flight Rules (VFR) versus Instrument Flight Rules (IFR)
- Availability and reliability of both hardware and software

Section 7 identifies sources of data to use in SRM.

Once the system elements are listed, a careful review of the NAS change description should be conducted. A bounded system limits the analysis and assessment to the components necessary to adequately determine the safety risk associated with the NAS change, system, and/or operation. When there is doubt about whether to include a specific element in the analysis, it is preferable to include that item, even though it might prove irrelevant during the hazard identification phase.

3.5.6.2 Considerations for Existing Safety Issues

Existing safety issues must clearly define the issue's scope using insights from data analysis and input from technical experts. To accomplish this, the existing safety issue description should include results from in-depth data analysis. These analyses may establish preliminary hazard elements including:

- Hazard descriptions,
- Causes,
- System states,
- Controls,
- Effects, and
- Initial/current risk levels

3.5.6.3 5M Model Method

The 5M Model must be used to capture the information needed to describe the system and aid in hazard identification. The 5M Model uses a Venn Diagram to depict the interrelationships among its five elements, as seen in Figure 3.5. To adequately bound and describe a system, it is important to understand the relationships between the elements of the 5M Model.

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

- **Mission:** The clearly defined and detailed purpose of the proposed NAS change or system/operation
- **(hu)Man/Person:** The human operators, maintainers, and affected stakeholders
- **Machine:** The equipment used in the system, including hardware, firmware, software, human-to-system interfaces, system-to-system interfaces, and avionics
- **Management:** The procedures and policies that govern the system’s behavior
- **Media:** The environment in which the system is operated and maintained

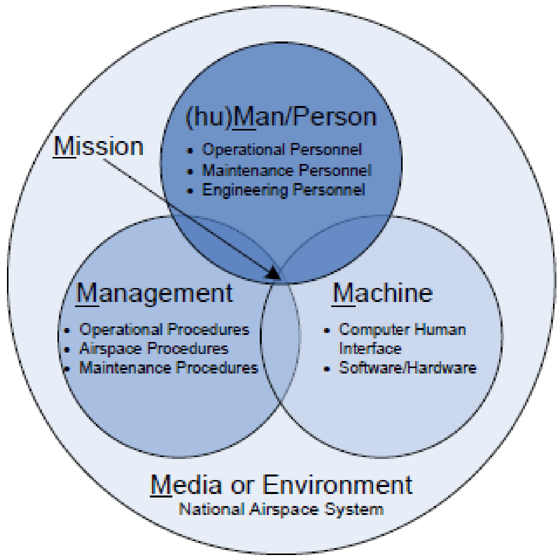


Figure 3.5: 5M Model

The 5M Model and similar techniques are used to deconstruct the proposed NAS change in order to distinguish elements that are part of or affected by the proposed NAS change. These elements later help to identify sources, causes, hazards, and current and proposed risk mitigation strategies.

3.6 DIAAT Phase 2: Identify Hazards

I	IDENTIFY HAZARDS	Identify hazards Use a structured approach Be comprehensive and do not dismiss hazards prematurely Employ lessons learned and experience supplemented by checklists

3.6.1 Overview

During the hazard identification phase, identify and document hazards, their possible causes, and corresponding effects. This phase is required to determine the appropriate means to address any safety risks associated with a NAS change or existing safety issue. A **hazard** is defined as any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. A hazard is a prerequisite to an accident or incident.

The following resources and methods can be used to identify hazards:

- The safety analysis that accompanies the proposed implementation of a new or modified operation, process, or piece of NAS equipment;
- Air Traffic Safety Action Program and Technical Operations Safety Action Program reports;
- AOV compliance audits;

- The Aviation Risk Identification and Assessment (ARIA) automated system;[5]
- National Transportation Safety Board safety recommendations;
- ATO Audits and Assessments;
- Audits performed as part of facility-level Quality Control efforts or AJI Quality Assurance efforts; and
- Reports of unsafe conditions in daily operations.

Refer to Section 6 for information about the various audit and reporting programs and tools.

3.6.2 Potential Sources of Hazards

The hazard identification stage considers all possible causes of hazards. The use of previous hazard analyses when identifying hazards is important, as it provides consistency in SRM and can reduce the time needed to identify hazards. For example, approved SRM documents on similar NAS changes or earlier integrated assessments, including applicable cross-organizational safety assessments and Independent Operational Assessments (IOAs), may be useful. Refer to Section 6 for information on IOAs.

Depending on the nature and size of the system under consideration, the causes may include:

- NAS equipment failure/malfunction,
- Operating environment (including physical conditions, airspace, and air route design),
- Human operator failure/error,
- Human-machine interface problems,
- Operational procedures limitations/design,
- Maintenance procedures limitations/design, and/or
- External services.

3.6.3 Existing Hazards

An existing hazard is any hazard that is currently in the NAS. Existing hazards often fall into the following categories.

3.6.3.1 Hazards Identified but Not in the Scope of an Ongoing NAS Change

These hazards must typically be addressed through a separate, follow-on safety analysis performed by the organization deemed responsible. An AJI SCL can assist in determining which organization should be notified about the existing hazard(s) identified.

3.6.3.2 Hazards Identified by Audits

When an audit identifies a potential safety issue, the issue must be addressed. Refer to FAA Order JO 2900.2, *Air Traffic Organization Audits and Assessments*.

3.6.3.3 Emergency Modifications

There may be unusual, unforeseen, or extraordinary issues or conditions that require the implementation of hardware or software solutions in a timeframe that does not allow proceeding through the formal SRM process. Emergency modifications are temporary fixes installed to maintain continuity of air navigation, air traffic control, communications, or support services

5. FAA Order JO 7210.633, *Air Traffic Organization Quality Assurance (QA)*, removed Risk Analysis Events (RAEs) and Risk Analysis Process (RAP), the process for notification and interviews associated with RAE. Any references to RAEs or RAP in this SMS Manual are for research and historical purposes only.

during unusual or emergency conditions. Such NAS changes may result from unforeseen natural occurrences, a lack of replacement parts, software patches, or real-time situations that require immediate action. Refer to FAA Order 6032.1, *National Airspace System (NAS) Modification Program*, for more information on emergency modifications.

A memorandum must be sent to the Director of Policy and Performance, AJI-3, within two days of the implementation of the modification.[7]

The memorandum must:

- State what system was modified,
- Provide a summary of the emergency modification,
- Identify why the modification was made, and
- Indicate when the safety risk assessment will be conducted.

The official who authorized the emergency modification must ensure that SRM is performed in accordance with the ATO SMS Manual within 30 days of the implementation of the modification. After SRM is completed, a follow-up memorandum must be sent to the AJI-3 Director stating that it has been completed and uploaded to the SMTS. The AJI-3 Director must inform AOV and the ATO Chief Operating Officer (COO).

3.6.3.4 Existing High-Risk Hazards

If an existing high-risk hazard is identified:

1) The responsible/affected Service Unit must send supporting data and documentation of the existing high risk to AJI-3 for validation.
2) AJI-3 must review and validate whether the identified hazard qualifies as high risk. For additional information on this process, contact AJI-3 via the ATO SMS mailbox.
3) The AJI-3 Director must notify the ATO COO and AOV via memorandum of the validated existing high-risk hazard and the interim mitigations needed to mitigate the risk.
4) The ATO COO must either accept the interim mitigations and the associated risk **or** require the operation to stop.
5) Thirty calendar days after the notification is sent to the ATO COO and AOV, the responsible Service Unit in coordination with AJI-3 must conduct further SRM analysis and develop a permanent plan that will eliminate the hazard or reduce the risk to an acceptable level.
6) The existing high-risk hazard, along with all identified mitigations (both interim and permanent) to lower the risk to an acceptable level, must be captured in an SRM document.

7. The AJI-3 Director provides leadership and expertise to ensure that operational safety risk in the air traffic services that the ATO provides is identified and managed. They also ensure that safety risk is considered and proactively mitigated in the early development, design, and integration of solutions.

7) The SRM document must be written in accordance with the documentation requirements contained in this SMS Manual (see Annex A, Section 3.2) and be uploaded to SMTS within 30 calendar days of implementing the final safety requirements.

3.6.4 Elements of Hazard Identification

When considering new NAS equipment and procedures or planned modifications to current NAS equipment and procedures, define the data sources and measures necessary to identify hazards. The elements of a thorough system description contain the potential sources of hazards associated with the proposed NAS change. There are numerous ways to do this, but all require at least three elements:

- Operational expertise that relates specifically to the operation or equipment,
- Training or experience in various hazard analysis techniques, and
- A defined hazard analysis tool.

3.6.4.1 Tools and Techniques for Hazard Identification

In many cases, to identify safety hazards, a Preliminary Hazard List (PHL) and the required Hazard Analysis Worksheet (HAW) will suffice. If an additional means to identify hazards and compare solutions is required, select the methodology that is most appropriate for the type of system being evaluated. The Service Center and/or an AJI SCL can provide additional guidance on which tool(s) to use for various types of NAS changes.

When selecting hazard identification/analysis tools, it is important to consider:

- The necessary information and its availability;
- The timeliness of the necessary information;
- The amount of time required to conduct the analysis; and
- The tool that will provide the appropriate systematic approach for:
  - Identifying the greatest number of relevant hazards,
  - Identifying the causes of the hazards,
  - Predicting the effects associated with the hazards, and
  - Assisting in identifying and recommending risk management strategies.

Table 3.1: Hazard Identification Tools and Techniques

Analysis Tool/Technique	Summary Description
PHL / What-If Analysis	The PHL / What-If Analysis methodology identifies hazards, hazardous situations, or specific accident events that could produce an undesirable consequence. One can use the PHL / What-If Analysis as a brainstorming method. The PHL / What-If Analysis may be a combination of hazards, causes, effects, and system states. The items listed in the PHL / What-If Analysis all have the potential to be placed into the HAW.
Failure Mode and Effect Analysis	The Failure Mode and Effect Analysis determines the results or effects of sub-element failures on a system operation and classifies each potential failure according to its severity.

Analysis Tool/Technique	Summary Description
Failure Modes, Effects, and Criticality Analysis	The Failure Modes, Effects, and Criticality Analysis is an essential function in design from concept through development. The Failure Modes, Effects, and Criticality Analysis is iterative to correspond with the nature of the design process itself. It identifies component and sub-system failure modes (including the effect of human error), evaluates the results of the failure modes, determines rates and probability, and demonstrates compliance with safety requirements.
Fault Hazard Analysis	The Fault Hazard Analysis is a deductive method of analysis that can be used exclusively as a qualitative analysis or, if desired, can expand to a quantitative one. The Fault Hazard Analysis requires a detailed investigation of sub-systems to determine component hazard modes, causes of these hazards, and resultant effects on the sub-system and its operation.
Fault Tree Analysis	A Fault Tree Analysis 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. It is used to model faults in terms of failures, anomalies, malfunctions, and human errors.
Job Task Analysis	The foundation of the performance of a Human Error Analysis is a Job Task Analysis, which describes each human task and subtask 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. The Job Task Analysis should also identify the skills and information required to complete tasks; equipment requirements; the task setting, time, and accuracy requirements; and the probable human errors and consequences relating to these areas. There are several tools and techniques for performing task analyses, depending on the level of analysis needed.
Operational Hazard Assessment (OHA)	The OHA is a qualitative severity assessment of the hazards associated with the system. The OHA includes tabular worksheets and the PHL.
Scenario Analysis	The Scenario Analysis tool identifies and corrects potentially hazardous situations by postulating accident scenarios in cases where it is credible and physically logical to do so.

3.6.5 Developing a HAW

When hazards are identified, the **HAW** is required as part of the ATO SRM process.[8] It is a tool used to provide an initial overview of the hazard's presence in the overall flow of the operation and is used both for Operations and Second-Level Engineering. When developing the HAW, it is crucial to consider the hazards inherent to all aspects of an operation without regard to risk. ATO safety professionals use the HAW in nearly all risk management applications, except in the most time-critical situations.

Using the HAW helps panels overcome the tendency to focus on safety risk in one aspect of an operation and overlook more serious issues elsewhere in the operation. Its broad scope guides the identification of issues that may require analysis and assessment with more detailed hazard identification tools. A HAW with complete and accurate information provides an effective overview of the hazard's presence within the overall flow of the operation and helps ensure the safety analysis does not focus on risk in just one aspect of an operation while overlooking

8. All SRM documentation containing findings with hazards (with the exception of the PSP, Operational Safety Assessment (OSA), the Comparative Safety Assessment, and System Safety Assessment Report) requires the use of a HAW. Worksheets specific to these documents are contained in the SRMGSA.

critical issues elsewhere. Refer to Annex A for a description of the expected contents of the HAW.

3.6.6 Causes and System State Defined

Identify and document potential safety issues, their possible causes, and the conditions under which the safety issues are revealed (i.e., the system state).

A **cause** is the origin of a hazard. Causes are events occurring independently or in combination that result in a hazard. Causes include, but are not limited to, human error, latent failure, active failure, design flaw, component failure, and software error.

A **system state** is the expression of the various conditions, characterized by quantities or qualities, in which a system can exist. A system state should account for predictable scenarios, and the probability of those scenarios must be considered when determining the likelihood of a hazard or its effect occurring. (See Section 3.7.4.3 for information regarding determining likelihood.) It is important to capture the system state that most exposes a hazard, while remaining within the confines of any operational conditions and assumptions defined in existing documentation. **Assumptions** are conclusions based on the presumed condition of a system or system state—not documented facts, desired outcomes, or mitigations. The system state can be described using a combination of the terms below. (This is not a complete list.)

- **Operational and Procedural:** VFR versus IFR, simultaneous procedures versus visual approach procedures, etc.
- **Conditional:** Instrument Meteorological Conditions (IMC) versus Visual Meteorological Conditions (VMC), peak traffic versus low traffic, etc.
- **Physical:** Electromagnetic environment effects, precipitation, primary power source versus back-up power source, closed runways versus open runways, dry runways versus contaminated runways, environmental conditions, etc.

Risk analyses and assessments must consider all possibilities while allowing for all system states. During the SRM process, the SRM panel must consider the probability of the identified system state(s) when determining the likelihood of a hazard's effect(s) and use that determination consistently throughout the analysis. This ensures clarity and aligns likelihood estimates with potential system state conditions. Any given hazard may have a different risk level in each possible system state.

3.6.7 Addressing Hazards that Cross FAA LOBs

FAA SRM policy provides risk management policy to follow when hazards, risks, and associated SRM affect multiple LOBs. The ATO must consider and, when necessary, use the provisions in this order when coordinating SRM with other FAA organizations. AJI will function as the ATO liaison to interface with organizations outside of the ATO when the provisions of FAA Order 8040.4 are invoked.

3.6.8 Hazard Escalation and Reporting

There may be cases in which the ATO and another FAA organization disagree on key issues surrounding a NAS change. The AJI-3 Director and the Safety Management Group, AJI-31, Manager must be made aware of such NAS changes and must work to determine the appropriate course of action. The AJI-3 Director will determine whether such hazards and issues need to be elevated to an FAA-level mediation process facilitated by the FAA SMS Committee.

For more information, refer to the FAA SMS Hazard Escalation Reporting Process.

3.7 DIAAT Phase 3: Analyze Risk

A	**ANALYZE RISK**	Identify controls Determine the severity and likelihood of the hazard's effect

3.7.1 Overview

An accident or incident rarely results from a single failure or event. Consequently, risk analysis is seldom a binary (e.g., on/off, open/closed, or broken/operational) process. Risk analyses can identify failures from primary, secondary, or even tertiary events; and they should consider credible combinations of causes, system state characteristics, control failures, and operational conditions when discussing hazards and their associated risk.

During the risk analysis phase:

- Evaluate each hazard (identified during the "Identify Hazards" phase) and the system state (from the "Describe the System" and "Identify Hazards" phases) to determine the controls,
- Analyze how the operation would function should the hazard occur, and
- Determine the hazard's associated severity and likelihood and provide supporting rationale.

3.7.2 Controls

A **control** is any means currently reducing a hazard's causes or effects. Policies, procedures, hardware, software, or other tools can only be considered controls if they are part of the operating NAS and have demonstrated effectiveness. Understanding controls affects the ability to determine credible effects. Certain controls may only be in place in certain operating environments or under certain system states. Do not document safety requirements as controls; safety requirements are planned or proposed ways to reduce risk. Refer to Section 3.9.3 for information about documenting safety requirements.

Provide supporting data and/or a rationale that confirms the control's use, applicability, and availability related to the hazard. For instance, if orders are identified as controls, cite the specific version, paragraph, and/or section number(s). Alternatively, if equipment is identified as a control, discuss how it reduces or manages the risk. Only document the controls associated with the NAS change under evaluation. When considering existing hazards identified through safety audits or post-event risk analyses, consider any control(s) that either minimized the hazard's effect or failed.

Table 3.2 provides broad examples of controls. This is not a comprehensive list of controls; each identified control should be directly applicable to the hazard being addressed.

Table 3.2: Examples of Controls

Controller	Pilot	Technical Operations
• Radar surveillance - Ground and airborne • Controller scanning - Radar - Visual (out window) • Conflict Alert, Minimum Safe Altitude Warning, Airport Movement Area Safety System (AMASS) • Procedures - Specific SOP reference - Order reference • Triple redundant radio • Controller intervention • Management oversight • Completed training	• Traffic Collision Avoidance System (TCAS) • Ground Proximity Warning System • Visual scanning (out window) • Radar surveillance • Checklists • Redundancies / back-up systems • Pilot intervention (evasive action)	• Preventive maintenance • Failure warnings / maintenance • Alerts • Redundant systems - Triple redundant radio - Software redundancy • Diverse points of delivery • Fall-back systems - Center radar processing • Software/hardware designs

3.7.3 Determining Credibility of a Hazard's Effect(s)

Effect refers to the real or credible harmful outcome that has occurred or can be expected to occur if the hazard occurs in the defined system state. A single hazard can have multiple effects. An effect is considered credible if it is reasonable to expect the effect to occur within the combination of conditions defining the system state, and within the lifetime of a typical ATC system (i.e., 30 years). Credible effects must be determined with respect to controls. All identified credible effects of a hazard must be documented.

Often, there is confusion when distinguishing the *possible* effects of a hazard from the *credible* effects; possible is not necessarily the same as credible. The credibility of an effect is a nuanced and key consideration in the analysis. A thorough understanding of this concept can save time in determining the risk level of a specific hazard. When determining the credibility of the effect, it is important to:

- **Recall and Understand the Defenses in Depth Model.** It is well established that incidents and accidents cannot typically be attributed to a single failure, or even to a single individual. Rather, aviation safety issues are the end result of a number of failures (causes or failures). Based on this model (see Section 2.5.1), it is critical to consider the defenses that already exist in the NAS when deciding the credibility of an effect.
- **Review History.** Check the historical record. Have there been similar NAS changes? What happened? How does the experience gained from the activities affect the credibility of the outcomes that have been identified for the NAS change?
- **Rely on Quantitative Data.** Section 3.7.4.3.3 and Section 3.7.4.3.4 discuss the use of quantitative and qualitative data, respectively. Do the quantitative data support the credibility of the outcomes identified? If so, the hazard severity determination can be based on statistical data, and the determinations of the SRM panel members will be

more objective. Section 7 provides additional information about the aviation safety databases available for gathering data.

- **Visualize the Occurrence of the Accident or Incident.** Put the hazard in its proper context within the given system state and determine the sequence of events (causes) that could lead to the worst credible outcome. Given that the ATO strives to build error-tolerant systems (in accordance with the Defenses in Depth Model), consider how many controls (redundancies, procedures, warning devices, equipment, etc.) would have to fail for an identified hazard to breach every defense to result in a catastrophic event. Is it credible to expect that the necessary combination of extreme conditions will simultaneously occur within the operational lifetime of the system?

3.7.4 Determining Risk

3.7.4.1 How to Determine Risk

Risk is the composite of predicted severity and likelihood of the potential effect of a hazard. While the worst credible effect may present the highest severity, the likelihood of this effect is often very low. A less severe effect may occur more frequently and therefore present a higher overall risk than the more severe effect. The ways to reduce the risk for the two effects may be different, and both must be identified. Consider all credible effects and their associated risks in order to identify the highest risk for the safety hazard.

Attempt to obtain and document objective evidence (e.g., historical evidence of similar NAS changes, testing data, modeling, or simulation results) to support the assessed level of risk. If quantitative data are not available, document the research methods—including the data sources reviewed—in addition to qualitative risk assessments. Because different system states can affect both severity and likelihood in unique ways, determine whether the hazard will exist in several system states and analyze the risk accordingly.

3.7.4.2 Determining Severity

Severity is the credible consequence or impact of a hazard's effect or outcome in terms of degree of loss or harm. It is independent of likelihood and must be determined before likelihood is calculated. A single hazard can have multiple effects. Assess the severity of each effect separately, considering existing controls. To justify the severity level, a detailed rationale must be provided in the HAW describing (1) how the identified effect could occur as a result of the proposed change / existing safety issue and (2) why the panel's severity determination for the effect is appropriate.

In situations where ATM/CNS services are not expected or when a NAS change or existing issue crosses FAA Lines of Business, consult with the affected line of business and follow the provisions of FAA Order 8040.4, *FAA Safety Risk Management (SRM)*. Where these services are expected, use the severity level criteria and the severity classification examples in Table 3.3 and Table 3.4 to assess the severity of each effect. (See Section 3.7.3 for additional guidance in determining credibility of hazard effects.)

3.7.4.2.1 Severity Level Criteria

The criteria below consider severity language and classifications from FAA Order 8900.1, *Flight Standards Information Management System*, Volume 7, and FAA Order 7050.1B, *Runway Safety Program*. Table 3.3 and Table 3.4 provide clarity of these criteria through detailed example effects specific to the type of operation.

- **Minimal.** Condition or occurrence/event that is unintended but has little to no impact on ATM or CNS services, and no immediate safety consequences
- **Minor.** Condition or occurrence/event that requires action/intervention by ATC, pilot, or other party (e.g., Technical Operations specialist, vehicle operator), but with ample time and/or distance to avoid an accident or incident; potential for an accident is low
- **Major.** Occurrence/event in which there is potential for an accident if no action is taken, necessitating a timely response (e.g., an ATC safety alert or vehicle/aircraft evasive maneuver), but the situation can be managed in enough time that an accident never becomes imminent
- **Hazardous.** Occurrence/event in which there is little to no time available to recognize the threat and react appropriately, and an accident is imminent without immediate action (e.g., a last-second evasive maneuver or emergency procedure; an accident is narrowly avoided by chance); or an accident occurs but does not result in fatality or substantial damage to the airframe
- **Catastrophic.** An accident with at least one fatality

3.7.4.2.2 Determining Severity of Effects on Air Traffic Services

The following table presents example effects and their typical severity classifications. When assessing severity, the assigned level must align with the criteria listed above. However, in some cases, the severity level may be lower or higher than the examples below due to additional controls that limit exposure or operational interactions/dependencies that increase exposure. A detailed rationale justifying the severity classification must be provided in the HAW.

Table 3.3: Severity Table for Example Effects

		Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
		CONDITIONS RESULTING IN ANY ONE OF THE FOLLOWING:				
Surface Effects for Manned Aircraft[1] / Vehicle	**Example ATC Effects**	**Category (CAT) D Runway Incursion (RI)[2]:** Incorrect presence of a single vehicle/person/aircraft on a surface designated for landing/take-off of aircraft, but with no immediate safety concerns	**CAT C RI[2]:** Ground incident in which there is ample time and/or distance to avoid a collision A ground incident in which an aircraft, vehicle, or pedestrian crosses the runway holding position marking (hold line) and causes a conflict with ground air traffic but stops more than 100 feet from the runway edge and requires no corrective/evasive response to avoid an accident (CAT C RI)	**CAT B RI[2]:** Ground incident in which separation decreases and there is a significant potential for collision, which may result in a corrective/evasive response to avoid a collision, but an accident never becomes imminent A ground incident or overflight in which both parties (aircraft and another aircraft or a vehicle/pedestrian) are within the edges of the runway and the closest unintended proximity remains no less than 2,000 feet horizontally and (for overflights) no less than 200 feet vertically (CAT B RI)	**CAT A RI[2]:** Ground incident in which a collision is narrowly avoided (e.g., collision was imminent but avoided by chance) A ground incident or overflight in which any part of an aircraft and another aircraft or vehicle/pedestrian are on or above the runway surface, and the closest unintended proximity is within 100 feet horizontally or vertically	Ground collision[3] with at least one fatality and/or substantial damage to airframe of manned aircraft Controlled flight into terrain or obstacles with fatality
	Example Flight Crew Effects	Circumstances causing a flight crew to reject or abort takeoff, but with no degradation of aircraft performance capability or other safety consequence Incorrect presence of a single vehicle/person/aircraft on a surface	Circumstances that result in the potential for a ground incident and lead a flight crew to abort or reject takeoff (aircraft performance capability not degraded); however, there is ample time and/or distance to avoid a collision	Circumstances causing a flight crew to abort or reject takeoff to avoid a ground incident, which results in degradation of aircraft performance capability Circumstances causing close enough ground proximity between	Circumstances causing narrowly avoided ground collision[3] (e.g., collision was imminent but avoided by chance) and there was no/late ATC detection/ intervention—or pilot intervention occurred prior to ATC detection/ intervention (CAT A RI)	Ground collision[3] with at least one fatality Controlled flight into terrain or obstacles with fatality

		Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
		CONDITIONS RESULTING IN ANY ONE OF THE FOLLOWING:				
Surface Effects for Manned Aircraft[1] / Vehicle		designated for landing/take-off of aircraft, but with no immediate safety concerns (CAT D RI)	Circumstances causing below-normal ground proximity between aircraft/ vehicles/ pedestrians, but with timely detection/ intervention by ATC / flight crew and ample time and/or distance to avoid a collision (CAT C RI) A ground incident in which an aircraft comes into conflict with another aircraft, vehicle, or pedestrian on the runway, but the proximity of the aircraft to the runway edge remains above 100 feet, and the pilot is not required to take corrective/evasive action to avoid an accident (CAT C RI)	aircraft/vehicles/pedestrians to require timely corrective actions or evasive maneuvers to avoid a ground collision[3] (CAT B RI), with no or late detection/intervention by ATC / flight crew, and high rate of closure A ground incident or overflight in which both parties (aircraft and another aircraft or a vehicle/ pedestrian) are within the edges of the runway and the closest unintended proximity remains no less than 2,000 feet horizontally and (for overflights) no less than 200 feet vertically. The pilot may be required to take timely corrective actions or evasive maneuvers to avoid an accident (CAT B RI)	A ground incident or overflight in which any part of an aircraft and another aircraft or vehicle/pedestrian are on or above the runway surface and the closest unintended proximity is within 100 feet horizontally or vertically Ground collision[3] that does not result in fatality	
Airborne Effects for Manned Aircraft	**Example ATC Effects**	Circumstances requiring ATC or flight crew to issue go-around instructions but with no immediate safety consequence Circumstances that lead to	**CAT C NMAC[4]:** Event in which airborne proximity between manned aircraft is below normal but above 500 feet, and there is timely ATC detection and intervention and ample time to avoid a collision	**CAT B NMAC[4]:** Event in which airborne proximity between manned aircraft is between 100 and 500 feet, with no or late detection and intervention by ATC, and high rate of closure,	**CAT A NMAC[4]:** Event in which airborne proximity between manned aircraft is less than 100 feet (collision narrowly avoided), with high rate of closure and no or late ATC detection/ intervention—or pilot intervention	Mid-Air Collision resulting in fatality Controlled flight into terrain or obstacles with fatality

		Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
		CONDITIONS RESULTING IN ANY ONE OF THE FOLLOWING:				
Airborne Effects for Manned Aircraft		airborne traffic conflict, but with no immediate threat of collision or other safety consequence		potential for collision	prior to ATC detection/ intervention. - - - - - Mid-air collision that does not result in fatality	
	Example Flight Crew Effects	Circumstances requiring ATC or flight crew to initiate a go-around / reject landing, but with no immediate safety consequence - - - - - Circumstances that lead to airborne traffic conflict, but with no reduced proximity, immediate threat of collision or other safety consequence - - - - - Pilot is aware of traffic (identified by TCAS traffic alert, issued by ATC, or observed by flight crew) in close enough proximity to require focused attention, but no action is required to avoid a collision, and there is no other safety consequence	Circumstances causing rejected landing or go-around that results in below-normal proximity between manned airborne, aircraft, but separation remains above 500 feet and there is timely ATC detection and mitigation and ample time to avoid a collision - - - - - **CAT C NMAC[4]:** Event in which at least one pilot was surprised by the proximity of the other; however, a collision is unlikely even if the pilot takes no evasive action, or there is ample time and/or distance to avoid a collision - - - - - Encounters between manned airborne aircraft with proximity of 500 feet or greater, or slowly converging flightpaths	**CAT B NMAC[4]:** Event of close proximity between airborne aircraft which could have resulted in a collision if no action had been taken by the pilot (no/late ATC detection or intervention), but a collision never becomes imminent - - - - - Encounters between manned airborne aircraft at between 100 and 500 feet separation - - - - - An event with close proximity (e.g., between 100 and 500 feet) with late detection/ intervention by controller or flight crew, and high rate of closure - - - - - An event that incites a TIS alert or TCAS RA, or an event with an out-the-window sighting of air traffic without electronic aid; the	**CAT A NMAC[4]:** Event of close proximity between airborne aircraft in which collision was narrowly avoided by chance, rather than by a pilot's evasive action (no/late detection or intervention by pilot or ATC) - - - - - Encounters between manned airborne aircraft with proximity below 100 feet - - - - - An event in which a last-second evasive maneuver or emergency procedure is necessary to avoid collision and/or situations where little or no time is available to recognize the threat and react appropriately; collision is imminent without immediate action - - - - - An event in which collision is narrowly avoided, there is a high rate	Mid-Air Collision resulting in fatality - - - - - Controlled flight into terrain or obstacles with fatality

		Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
	CONDITIONS RESULTING IN ANY ONE OF THE FOLLOWING:					
Airborne Effects for Manned Aircraft			An event that incites a TIS alert, TCAS Traffic Advisory (TA), or TCAS Resolution Advisory (RA); pilot responds to the inciting event after sighting the traffic with or without the aid of an electronic alert system, but no evasive maneuvers are required to avoid an accident, and proximity remains above 500 feet (***Note:*** This item assumes the alerts/advisories are not prompted by aircraft applying visual separation appropriately.)	inciting event leads the pilot to take timely corrective actions or conduct evasive maneuvers to avoid an accident. Proximity is between 100 and 500 feet (***Note:*** This item assumes the alerts/advisories are not prompted by aircraft applying visual separation appropriately.)	of closure, and no/late ATC detection/ intervention—or pilot must intervene prior to ATC detection/ intervention. Airborne collision that does not result in fatality	
Surface and Airborne Effects for UAS	**Example Surface and Airborne UAS Effects**	Circumstances that result in UAS operations outside of authorized conditions/areas, but there is no encounter with manned aircraft or other safety consequence Loss of UAS control, but there is no encounter with manned aircraft or other safety consequence	Circumstances requiring a manned aircraft to abort takeoff (i.e., rejected takeoff); however, the act of aborting takeoff does not degrade the aircraft performance capability or result in any other safety consequence Loss of UAS control leading to encounter with manned aircraft, but manned aircraft is not required to make evasive maneuvers to avoid the UAS, and UAS proximity	Circumstaces wherein a UAS crew has reduced ability to cope with adverse operating conditions and results in an encounter with a manned aircraft, but the UAS's proximity to manned aircraft remains greater than 500 feet Circumstances involving UAS that require a manned aircraft to abort takeoff (i.e., rejected takeoff), and the act of aborting takeoff degrades the aircraft	Manned aircraft making an evasive maneuver to avoid unmanned aircraft, and UAS proximity from unmanned aircraft is below 500 feet UAS collision with airborne manned aircraft, but with no fatality Circumstances requiring an airborne, manned aircraft to make an evasive maneuver to avoid a UAS, which results in a separate	A collision with a manned aircraft that causes fatal injury or death to manned aircraft occupants Proximity of UAS to manned aircraft that causes conditions preventing continued safe flight and landing of the manned aircraft, leading to a manned aircraft accident with fatality

	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
	CONDITIONS RESULTING IN ANY ONE OF THE FOLLOWING:				
Surface and Airborne Effects for UAS		to manned aircraft remains equal to or greater than 500 feet	performance capability Circumstances requiring a manned aircraft to make evasive maneuvers to avoid UAS, but the UAS's proximity to the manned aircraft remains equal to or greater than 500 feet, and there is no additional safety consequence Circumstances requiring an airborne, manned aircraft to make an evasive maneuver to avoid a UAS, which results in a separate encounter between two manned aircraft with proximity between 100 and 500 feet (CAT B NMAC between manned aircraft)	encounter between two manned aircraft with proximity of less than 100 feet (CAT A NMAC between manned aircraft) UAS encounter that causes a ground collision[3] between a manned aircraft and another manned aircraft or vehicle on the surface area, but with no fatality UAS encounter that causes collision between manned, airborne aircraft, but with no fatality	UAS encounter that causes collision between airborne manned aircraft resulting in fatality UAS encounter that causes a ground collision[3] between a manned aircraft and another manned aircraft or vehicle on the surface area, resulting in fatality

Notes:

1. Manned Aircraft. Aircraft with at least one person aboard (including flight crew / pilot).
2. Refer to FAA Order 7050.1, *Runway Safety Program*, for more information on runway incursions and other effects occurring on or near the operational movement area.
3. Ground Collision. An airplane on the ground collides with an object or person.
4. Refer to FAA Order 8900.1, *Flight Standards Information System*, Volume 7, for more information on NMACs and other airborne effects.

3.7.4.2.3 Determining Severity of Effects Related to NAS Systems/Equipment

SRM must be conducted throughout the AMS lifecycle in accordance with the SRMGSA and AMS policy on the FAA Acquisition System Toolset website. As such, the inherent functional severity of certain NAS equipment hazard effects has been analyzed and assessed.

When performing SRM on NAS equipment that was previously evaluated, it is recommended to use the data, methodology, and results of the previous work as the starting point for the new risk analysis. If there are differences in functionality between the original system and the system undergoing analysis, the differences should be accounted for and documented in the new risk analysis.

In general, NAS equipment can fail such that one of two effects is expected:

- **Loss of Function.** The service is unexpectedly unavailable.
- **Malfunction.** The service is being provided inaccurately or with diminished integrity.

When identifying functional failures that lead to hazards, the loss of function and the malfunction of constituent parts must be considered. The severity of malfunctions and losses of function from infrastructure systems, such as telecommunications and power systems, is dependent upon the services they support.

Examples of the systems that provide services include, but are not limited to, the following:

Navigation (NAV)

- *Instrument approach systems*: Localizer, glide slope (e.g., visual glide slope indicators, such as Precision Approach Path Indicator and Visual Approach Slope Indicator), Ground-Based Augmentation System, markers, approach lights, Distance Measuring Equipment (DME), Localizer-Type Directional Aid, and Runway Visual Range
- *En Route guidance systems*: Very-High Frequency Omnidirectional-Range Radio (VOR), Tactical Air Navigation, DME, and Wide-Area Augmentation System

Communication (COMM)

- Air-to-ground COMM: Headsets/microphones, speakers, voice switches, radio control equipment, and radios
- Ground-to-ground COMM: Headsets/microphones, speakers, and voice switches

Surveillance

- Automatic Dependent Surveillance – Broadcast (ADS-B), Airport Movement Area Safety System (AMASS), Automated Radar Terminal System (ARTS), Airport Surface Detection Equipment (ASDE), Air Route Surveillance Radar (ARSR), Air Traffic Control Radar Beacon System (ATCRBS), Mode Select Beacon System (MODES), Wide Area Multilateration (WAM), and Standard Terminal Automation Replacement System (STARS)

Weather

- Automated Surface Observing System (ASOS), Automated Weather Observing System (AWOS), Low-Level Wind Shear Alert System, Flight Service Automation System, Operations and Supportability Implementation System, Next Generation Weather Radar, Terminal Doppler Weather Radar, Weather and Radar Processor, and Weather Message Switching Center Replacement

3.7.4.2.4 Using NAS Equipment Effect Severity Examples

When determining the severity of hazards related to NAS equipment, refer to the example scenarios in Table 3.4. These are baseline examples for identifying potential operational impacts and on the NAS related to NAS system/equipment issues and determining severity of associated, credible effects. Table 3.4's examples of credible operational impact were:

- Previously derived from operational safety assessments and other documentation produced during initial safety assessments completed as part of the AMS processes that define severity based on the inherent functionality of systems and
- Reviewed/validated by a group of Subject Matter Experts (SMEs) in second-level engineering, air traffic management, SMS policy, and SRM panel facilitation

Operational impacts of specific NAS changes may vary (i.e., be better or worse) than the example scenarios in Table 3.4 if, for example, controls are present that limit exposure or there are interactions and dependencies that exist with other systems / within a specific system state. For this reason, credible effects may differ or be lower/higher in severity than Table 3.4 indicates. If the information in Table 3.4 does not fit a given scenario, Table 3.3 supplements example effects that occur in the NAS and can be used to help frame the severity analysis. (Additionally, see Section 3.7.3 for guidance in determining credibility of hazard effects.) Effect severity should be determined with regard to operational impact on the provision of ATM/CNS services.

Note: Losses in equipment functionality and equipment malfunctions may not necessarily be traceable to a loss in separation; therefore, losses of separation should be addressed independently.

Table 3.4: NAS Equipment Severity Examples

Service	Functionality	Failure Condition	Environment / System State	Example Credible Operational Impacts (***Note:*** Impacts may be better or worse depending on the details of the existing safety issue or proposed change)	Associated Severity
NAV	Instrument approach guidance	Loss of function	VMC	Pilot has to take over manual control, but there is little to no effect on the provision of ATM or CNS and no other safety consequence	Minimal or no safety impact
			IMC, non-critical phase of flight (i.e., outside of final approach fix)	Missed approach leading to airborne incident, but proximity remains above 500 feet, and there is ample time and/or distance to avoid collision (CAT C NMAC)	Minor
			IMC, critical phase of flight (i.e., near or immediately after touchdown)	Insufficient reaction time for pilot to execute missed approach, resulting in airborne incident with high rate of closure and proximity less than 100 feet; narrowly avoiding collision (CAT A NMAC)	Hazardous
		Malfunction	Day, VMC	Misleading Information is detected by flight crew and requires flight crew to continue with a visual approach, but with no other safety consequence	Minimal or no safety impact
			Night, VMC	An aircraft operates in closer proximity to obstacles/terrain than the instrument approach path was designed to allow, but no evasive maneuvers or corrective actions are required to avoid collision with obstacles/terrain The aircraft operates at an unexpected altitude during approach operations, which leads to below-normal proximity between aircraft, but proximity remains above 500 feet, and there is ample time or distance to avoid a collision (CAT C NMAC)	Minor

Service	Functionality	Failure Condition	Environment / System State	Example Credible Operational Impacts (*Note:* Impacts may be better or worse depending on the details of the existing safety issue or proposed change)	Associated Severity
NAV NAV (cont.)	Instrument approach guidance (cont.)	Malfunction (cont.)	Night, VMC (cont.)	An aircraft operates in closer proximity to obstacles/terrain than the instrument approach path was designed to allow, leading to an airborne incident requiring timely corrective actions or evasive maneuvers to avoid collision with another aircraft (proximity between 100 and 500 feet – CAT B NMAC) or with obstacles/terrain; however, collision never becomes imminent	Major
			IMC	Misleading information exceeds performance thresholds and leads to an airborne event in which a collision with another aircraft or with obstacles/terrain is narrowly avoided (e.g., proximity between aircraft is below 100 feet – CAT A NMAC)	Hazardous
				Misleading information provided to flight crew, leading to aircraft collision with another aircraft or with obstacles/terrain with a fatality or substantial damage to the airframe	Catastrophic
	Visual glide slope indicators (Precision Approach Path Indicator / Visual Approach Slope Indicator)	Loss of function	Night, VMC	Pilots must conduct visual operation without the Visual Glide Slope Indicator but there is no other safety consequence	Minimal or no safety impact
		Malfunction	Night, VMC	Misleading information leads pilot to operate at an inappropriate altitude during approach, which results in aircraft operating in closer proximity to obstacles/terrain than the approach path was designed to allow, but no evasive maneuvers or corrective actions are required to avoid collision with obstacles/terrain	Minor
	ILS glide slope	Loss of function	IMC	Missed approach but with no other safety consequence	Minimal

Service	Functionality	Failure Condition	Environment / System State	Example Credible Operational Impacts (***Note:*** Impacts may be better or worse depending on the details of the existing safety issue or proposed change)	Associated Severity
NAV (cont.)	ILS glide slope (cont.)	Malfunction	IMC	Misleading information leads pilot to operate at an unintended altitude, resulting in an aircraft accident or CFIT	Catastrophic
	En route guidance (e.g., VOR/DME)	Loss of function	IMC	Pilot transitions to alternate navigation method, but there is no further impact on safety	Minimal or no safety impact
		Malfunction	IMC	Misleading information leads to aircraft operating at unexpected/ inappropriate En Route altitude or flight path. This leads to a situation that requires timely corrective actions or evasive maneuvers to avoid an accident (CAT B NMAC); however, an accident never becomes imminent (proximity between 100 and 500 feet)	Major
	Runway visual range	Loss of function / malfunction	IMC	Missed approach, but with no other safety consequence	Minimal
COMM	Air-to-ground	Loss of single frequency	IMC and low to normal traffic volume, **or** VMC and low to high traffic volume	Pilot must switch to an alternate frequency, but there is no other safety impact	Minimal or no safety impact
				Pilots and ATC unable to communicate on that frequency, resulting in conflict between airborne aircraft, but with ample time/distance to avoid a collision (proximity remains greater than 500 feet)	Minor
			IMC, high traffic volume	Pilots and ATC unable to communicate on that frequency, resulting in an airborne traffic conflict that requires the pilot to make timely corrective actions or evasive maneuvers to avoid a collision (CAT B NMAC); however, a collision never becomes imminent (proximity between 100 and 500 feet)	Major

Service	Functionality	Failure Condition	Environment / System State	Example Credible Operational Impacts (***Note:*** Impacts may be better or worse depending on the details of the existing safety issue or proposed change)	Associated Severity
COMM (cont.)	Air-to-ground (cont.)	Simultaneous loss of multiple frequencies	IMC/VMC, Low to normal traffic volume	Pilots and ATC unable to communicate on multiple frequencies, resulting in an aircraft incident where timely corrective actions or evasive maneuvers are required to avoid a collision; however, a collision never becomes imminent (proximity between 100 and 500 feet)	Major
			IMC/VMC, High traffic volume	Pilots and ATC unable to communicate on multiple frequencies, resulting in an aircraft incident where an accident is narrowly avoided (proximity below 100 feet), or resulting in a non-fatal accident with no substantial damage to the airframe (cont.)	Hazardous
	Ground-to ground	Loss of function	All traffic conditions	ATC notices communication is not available and transitions to alternative communication, resulting in ground conflict between aircraft or aircraft and vehicles/pedestrians, but no evasive maneuvers or corrective actions are required to avoid a collision (CAT C RI)	Minor
Surveillance	Aircraft and vehicle position on surface	Loss of function	Low traffic volume	ATC loss of situational awareness resulting in ground conflict, but no evasive maneuvers or corrective actions are required to avoid a collision (CAT C RI)	Minor
			High traffic volume	ATC loss of situational awareness resulting in ground conflict wherein pilot must conduct timely corrective actions or evasive maneuvers to avoid collision (e.g., CAT B RI); however, a collision never becomes imminent (proximity between 100 and 500 feet)	Major
		Malfunction	All operational conditions	ATC makes decisions based on misleading information, resulting in ground conflict wherein pilot must timely corrective actions or evasive maneuvers to avoid collision (e.g., CAT B RI); however, a	Major

Service	Functionality	Failure Condition	Environment / System State	Example Credible Operational Impacts (*Note:* Impacts may be better or worse depending on the details of the existing safety issue or proposed change)	Associated Severity
Surveillance (cont.)	Aircraft and vehicle position on surface (cont.)	Malfunction	All operational conditions (cont.)	collision never becomes imminent (proximity between 100 and 500 feet)	Major (cont.)
	Airborne aircraft position	Partial loss of function (e.g., alternative info sources available)	All operational conditions	ATC loss of ability to determine position of airborne aircraft, but there is ample time/distance between aircraft to transition to the appropriate configuration to continue operations, and there is no other safety consequence.	Minimal
				ATC loss of ability to determine position of airborne aircraft, which leads to airborne conflict, but there is ample time/distance between aircraft to transition to the appropriate configuration to continue operations, and proximity remains above 500 feet (e.g., CAT C NMAC)	Minor
		Full loss of function (e.g., no alternative info sources available)	All operational conditions	ATC loss of ability to determine position of airborne aircraft, resulting in airborne conflict wherein the pilot must conduct timely corrective actions or evasive maneuvers to avoid collision (e.g., CAT B NMAC); however, collision never becomes imminent (proximity between 100 and 500 feet)	Major
		Malfunction	All operational conditions	ATC makes decisions based on incorrect aircraft position information, resulting in airborne conflict wherein the pilot must conduct timely corrective actions or evasive maneuvers to avoid collision (e.g., CAT B NMAC); however, collision never becomes imminent (proximity between 100 and 500 feet)	Major
	Identification Data for Airborne Aircraft	Loss of function	All operational conditions	ATC loses the ability to differentiate among aircraft, leading to an airborne conflict but there is ample time/distance between aircraft to transition to the appropriate configuration to continue operations and proximity	Minor

Service	Functionality	Failure Condition	Environment / System State	Example Credible Operational Impacts (***Note:*** Impacts may be better or worse depending on the details of the existing safety issue or proposed change)	Associated Severity
Surveillance (cont.)	Identification Data for Airborne Aircraft (cont.)	Loss of function (cont.)	All operational conditions (cont.)	remains equal to or above 500 feet (e.g., CAT C NMAC)	Minor (cont.)
		Malfunction	All operational conditions	ATC makes decisions based on incorrect aircraft identification information, resulting in air conflict wherein pilot must conduct timely corrective actions or evasive maneuvers to avoid collision (e.g., CAT B NMAC); however, a collision never becomes imminent (proximity between 100 and 500 feet)	Major
	Identification Data for Aircraft on Surface	Loss of function	All operational conditions	ATC loses the ability to differentiate among aircraft, which may result in inconvenience to ATC or operations on operational surface, but there is no other safety consequence	Minimal
		Malfunction	All operational conditions	ATC loses the ability to differentiate among aircraft, which may affect the quality of ATC services provided to traffic on operational surface and lead to a ground conflict between aircraft or between aircraft and vehicles/pedestrians, but no evasive maneuvers or corrective actions are required to avoid a collision (e.g., CAT C RI)	Minor
	Alerts	Loss of function	All operational conditions	ATC not alerted when aircraft exceed established safety parameters, delaying detection of an air or ground conflict and lead to an event wherein the pilot must conduct timely or corrective/evasive maneuvers to avoid collision (e.g., CAT B RI or CAT B NMAC); however, collision never becomes imminent (proximity between 100 and 500 feet)	Major
		Malfunction (i.e., false alarms)	All operational conditions	Alerts falsely alert pilots or ATC to aircraft position, causing an operational nuisance but with no safety consequence	Minimal or no safety impact

Service	Functionality	Failure Condition	Environment / System State	Example Credible Operational Impacts (***Note:*** Impacts may be better or worse depending on the details of the existing safety issue or proposed change)	Associated Severity
Surveillance (cont.)	Interfacility data	Loss of function	Low to normal traffic volume	ATC has a loss of automated coordination of airborne operations (e.g., handoffs and point-outs) and must transition to manual ATC methods; this increases the ATC operational complexity, but there is no other safety consequence.	Minimal or no safety impact
			High traffic volume	ATC has a loss of automated coordination of airborne operations (e.g., handoffs and point-outs) and must transition to manual ATC methods; this increases the ATC operational a short time and can allow aircraft to operate with reduced separation proximity remains above 500 feet, and there is ample time/distance to avoid a collision (e.g., CAT C NMAC)	Minor
Weather	Adverse weather information (includes wind shear, thunderstorms, icing, IMC, etc.)	Loss of function	All operational conditions	Adverse weather information reported as unavailable, leading to flight crew inconvenience (e.g., pilot must alter flight route), but there is no other safety consequence	Minimal or no safety impact
		Malfunction: failure to detect or detection in wrong location	All operational conditions	Adverse weather not reported, resulting in a situation wherein the pilot must conduct timely or corrective/evasive maneuvers to avoid an accident (CFIT or collision with obstacles); however, an accident never becomes imminent	Major
		Malfunction: false weather alerts	All operational conditions	Weather is falsely reported as adverse, leading to flight crew inconvenience/nuisance, but there is no other safety consequence	Minimal or no safety impact

3.7.4.3 Determining Likelihood

3.7.4.3.1 Likelihood versus Frequency

Likelihood is an estimation, in quantitative or qualitative terms, of the probability that a hazard's effect or outcome will occur. Likelihood may be informed by observed frequency where sufficient data exists. **Frequency** is the observed rate at which a given effect occurs and is generally determined through monitoring, operational data, or residual risk information. (See Section 4.3.1 for information on monitoring and current risk and Section 4.3.4 for information on residual risk.) Frequency may be used to assess current or residual risk, while likelihood estimates are used to assess initial risk and predicted residual risk when frequency cannot be determined. **Likelihood** is defined as the estimated probability or frequency, in quantitative or qualitative terms, of a hazard's effect or outcome. More specifically, the concept of likelihood can be separated into two components: likelihood/probability and frequency. **Frequency** is an expression of how often a given effect occurs; it is a known value determined (for example) by monitoring a hazard and its effects to identify initial, current, or residual risk (see Section 4.3.1 and Section 4.3.4). Conversely, likelihood is an expression of the probability of a hazard's effects occurring (i.e., a rate of how often a given effect is expected to occur), which is used to estimate initial and predicted residual risk. Provide a rationale for likelihood estimations in the HAW.

3.7.4.3.2 What to Consider When Defining Likelihood

Frequency and Modeling

Frequency is sometimes used to help estimate likelihood, but historical data do not always represent future conditions. Historical frequency may be zero for a given procedure, but that does not mean that the future likelihood is also zero. For example, a facility may conduct a procedure that has unreported incidents that could lead to an undesirable outcome, such as a loss of separation or a collision. Likewise, a facility may not have encountered the scenario or system state that exposes the more severe outcome. Consider all potential effects that are derived from indicators of the operation in all credible scenarios. This practice is required to challenge the philosophy of, "It has not happened in the past, so it will not happen in the future."

When possible, use modeling to examine the effects of hazards that are too rare to have significant historical statistical data available.[11] If modeling is required and data are available, the risk analysis should be based on statistical or observational data (e.g., radar tracks). Where there are insufficient data to construct statistical risk assessments, input from SRM panel members and SMEs can be used. This means that if the true rate of a particular type of operation is unknown, it can be estimated using expert judgment. It is important to note that complex proposed NAS changes, such as changes to separation standards, require quantitative data to support the associated risk analysis.

Credible Effects and Controls

Analyze the likelihood of all credible effects to: (1) Determine the highest potential risk and (2) Identify all system states that expose the risk. Remember that less severe effects may occur more frequently, producing a higher risk; this is why it is important to determine the likelihood of all credible effects. Consider controls when determining likelihood because they may minimize the likelihood of an effect.

Crossing FAA LOBs

When a NAS change crosses FAA LOBs, consult with the affected parties; FAA SRM policy applies.

3.7.4.3.3 Calculating Likelihood with Quantitative Data

Once the credible effects and the estimated rates of occurrence have been determined, it is possible to calculate a likelihood rating. The Operations Network database is the official source of NAS air traffic operations data.

11. For guidance on how to design and conduct modeling in support of safety risk analyses, refer to AOV Safety Oversight Circular 07-05A, *Guidance on Safety Risk Modeling and Simulation of Hazards and Mitigations*.

To estimate the likelihood, first determine the expected number of times the credible effect will occur (i.e., the number of times that the hazard will occur in the system state that will expose the risk). Then, divide that value by the number of ATO operations, flight hours, or operational hours in which the effect is exposed (i.e., the number of ATO operations, flight hours, or operational hours affected by the proposed NAS change or the existing hazard). Finally, compare the result of this calculation (presented below) to the ranges presented in Table 3.5 to determine the likelihood rating.

$$\textbf{Likelihood} = \frac{\text{Expected number of occurrences of } \textbf{the effect}}{\text{Known number of } \textbf{affected operations}}$$

Identify which likelihood unit to use to analyze the effect's maximum exposure rate (i.e., the number of ATO operations, flight hours, or operational hours). For example, for the following environments, the number of ATO operations will often be the most appropriate likelihood unit to use when analyzing the exposure of an effect: a Terminal Radar Approach Control (TRACON) facility; ARTCC with small, busy sectors; or an ATCT. However, when determining occurrences of an effect in the Oceanic domain or for an ARTCC with a larger sector, often the number of flight hours may be more appropriate. System acquisitions or modifications will use units of operational hours. Whether the NAS change applies to a single facility or to an entire NAS domain, it is important to use the relevant number of ATO operations in which the hazard may occur when calculating likelihood.

Table 3.5: Likelihood of the Effect Standards – ATO Operations and NAS Equipment

	Operations: Expected Occurrence Rate (per operation / flight hour / operational hour[12])	
	Quantitative (ATC / Flight Procedures / Systems Engineering)	
	LESS THAN	**GREATER THAN OR EQUAL TO**
Frequent A		1×10^{-3} (1 per 1,000)
Probable B	1×10^{-3} (1 per 1,000)	1×10^{-5} (1 per 100,000)
Remote C	1×10^{-5} (1 per 100,000)	1×10^{-7} (1 per 10,000,000)
Extremely Remote D	1×10^{-7} (1 per 10,000,000)	1×10^{-9} (1 per 1,000,000,000)
Extremely Improbable E	1×10^{-9} (1 per 1,000,000,000)	1×10^{-14} (1 per 100,000,000,000,000)

The values in Table 3.5 are derived from an analysis of historical ATC data mapped to the established engineering standard (Advisory Circular 25.1309-1, *System Design and Analysis*) and can be applied to both ATC and Flight Procedures. The ratios binding each expected occurrence rate range were determined through calculations made using ten years of aviation data. In each calculation, the numerator was the number of occurrences of a given severity level occurring during a ten-year period, as obtained from various relevant databases. The denominator was the number of ATO operations (or flight hours) in that ten-year period, as obtained through the Operations Network database or the National Transportation Safety Board

12. It is important to note that the close correlation between flight hours and operations is entirely coincidental; average flight time is roughly two hours, and each flight has about two Tower and two TRACON operations. The two numbers are not interchangeable.

database. The value was adjusted to reflect a forecast air traffic increase. A cut-off limit of 10^{-14} was established to define the boundaries of credible events for the purposes of calculating likelihood. Figure 3.6 depicts the likelihood continuum and the expected occurrence rate ranges.

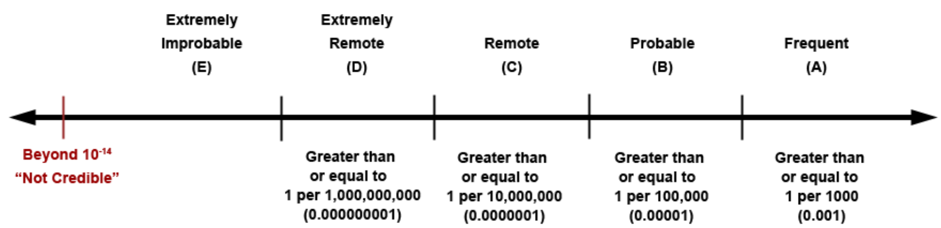


Figure 3.6: Likelihood Continuum

3.7.4.3.4 Determining Likelihood When No Data Are Available

For some NAS changes, the necessary data are not available. There may not be a similar enough change/procedure/situation in the NAS to provide similar data from which to estimate a rate of occurrence. When unable to use modeling, SME input can be utilized by SRM panel members to provide a qualitative approach to determine likelihood. This approach is only recommended when all avenues of data collection have been exhausted or when the change proponent is attempting to implement a new operation for which no data exist. For a majority of changes to the NAS, data from a similar NAS change may be collected and analyzed to determine the number of expected occurrences of an effect.

Table 3.6 presents calendar-based approximations of NAS-wide effect occurrences. This table only applies if the proposed NAS change or existing hazard affects all ATO operations in a particular air traffic domain.

Table 3.6: Calendar-Based Likelihood of the Effect Definitions – Operations/Domain-Wide

	Operations: Expected Occurrence Rate (Calendar-based)
	(Domain-wide: NAS-wide, Terminal, or En Route)
Frequent A	Equal to or more than once per week
Probable B	Less than once per week and equal to or more than once per three months
Remote C	Less than once per three months and equal to or more than once per three years
Extremely Remote D	Less than once per three years and equal to or more than once per 30 years
Extremely Improbable E	Less than once per 30 years

3.8 DIAAT Phase 4: Assess Risk

A	ASSESS RISK	Assign risk level for each hazard based on severity and likelihood

3.8.1 Overview

In this phase, identify each hazard's associated initial risk and plot each hazard on a risk matrix.

When assessing and mitigating safety risk, first determine the risk level prior to the implementation of any safety requirements (see Section 3.9.3). **Initial risk** describes the composite of the severity and likelihood of a hazard's effect, considering only controls and documented assumptions for a given system state. It describes the risk before any of the proposed mitigations are implemented.

When analyzing and assessing NAS equipment or existing hazards, the initial risk may be equated to the **current risk**, which is defined as the composite of severity and frequency of a hazard's effects in the present state.

3.8.2 Risk Levels and Definitions

Record all hazards and their associated risk levels. Hazards are assigned one of three risk levels: high, medium, or low. The ATO and its employees are responsible for identifying and mitigating hazards with unacceptable risk (i.e., high risk). Likewise, the ATO should determine if hazards with acceptable risk (i.e., medium and low risk) can be further mitigated.

3.8.2.1 High Risk

This is unacceptable risk, and the NAS change cannot be implemented unless the hazard's associated risk is mitigated to medium or low. Existing high-risk hazards also must be reduced to medium- or low-risk hazards. The predicted residual risk must be monitored and tracked in relation to the safety performance targets. The predicted residual risk must be confirmed with objective evidence suggesting an impact on the hazard's causes or effects.

Hazards with catastrophic effects that are caused by single point failures, common cause failures, or undetectable latent events in combination with single point or common cause failures are considered high risk, even if the possibility of occurrence is extremely improbable.

When a system has a **single point failure**, there is a failure of one independent element of the system that causes or could cause the whole system to fail. The system does not have a back-up, redundancy, or alternative procedure to compensate for the failed component. An example of a single point failure is found in 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 entire system will fail.

A **common cause failure** is a failure that occurs when a single fault results in the corresponding failure of multiple system components or functions. An example of a common cause failure is found in a system with redundant computers running on the same software, which is susceptible to the same software bugs.

3.8.2.2 Medium Risk

Although initial medium risk is acceptable, it is recommended and desirable that safety requirements be developed to reduce severity and/or likelihood. The risk must be monitored and tracked in relation to the safety performance targets. The predicted residual risk must be confirmed with objective evidence suggesting an impact on the hazard's causes or effects. Refer to Section 4.2 for information on monitoring.

A catastrophic severity and corresponding extremely improbable likelihood qualify as medium risk, provided that 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 hazard is categorized as high risk.

3.8.2.3 Low Risk

This is acceptable risk without restriction or limitation. It is not mandatory to develop safety requirements for low-risk hazards; however, develop a monitoring plan with at least one safety performance target.

3.8.3 Plotting Risk for Each Hazard

The risk matrix shown in Figure 3.7 is used to determine risk levels. Plotting the risk for each hazard on the matrix helps to prioritize treatment. The rows in the matrix reflect the likelihood categories, and the columns reflect the severity categories. Adhere to the following guidelines when plotting risk for each hazard:

- Plot a hazard's risk according to its associated severity and likelihood.
- To plot the risk for a hazard on the risk matrix, select the appropriate severity column (based on the severity examples in Table 3.3) and move down to the appropriate likelihood row (based on the likelihood definitions used from either Table 3.5 or Table 3.6).
- Plot the hazard in the box where the severity and likelihood of the hazard's effect intersect.
- If the plotted 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. As shown in the split cell in the bottom right corner of the matrix, hazards with a catastrophic severity and extremely improbable likelihood can be medium or high risk, depending on the cause, as explained in Section 3.8.2.1.

Use this SMS Manual and the risk matrix in Figure 3.7 for all SRM panels in which the ATO accepts the risk. When an FAA LOB other than the ATO is required to accept the safety risk, FAA Order 8040.4, and the risk matrices therein, apply. FAA Order 8040.4 also applies with regard to acceptability of risk levels at the agency level when crossing LOBs.

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

*Risk is high when there is a single point or common cause failure.

Figure 3.7: Risk Matrix

3.9 DIAAT Phase 5: Treat Risk

T	TREAT RISK	Choose risk management strategies Develop safety performance targets Develop monitoring plan

3.9.1 Overview

In this phase, identify appropriate means to mitigate or manage the safety risk. Treating risk involves:

- Identifying appropriate safety requirements,
- Defining safety performance targets or a sound alternate method to verify the predicted residual risk for each hazard, and
- Developing a monitoring plan that prescribes tasks and review cycles for comparing the current risk to the predicted residual risk.

3.9.2 Risk Management Strategies

To address safety risk, identify and evaluate means that either manage the risk or reduce it to an acceptable level. The four risk management strategies are risk control, risk avoidance, risk transfer, and risk assumption. Assess how the proposed risk management strategy affects the overall risk. Consider using a combination of actions to best manage or reduce the risk to an acceptable level.[13] When determining the appropriate strategy, consider how the safety

13. Refer to Section 2.8 for information about the Safety Order of Precedence.

performance target (see Section 4.1) will be used to evaluate the safety performance of the chosen course of action.

3.9.2.1 Risk Control

A **risk control strategy** involves the development of **safety requirements**, defined as planned or proposed means to reduce a hazard's causes or effects. Examples include policies or procedures, redundant systems and/or components, and alternate sources of production. Refer to Section 3.9.3 for information on documenting safety requirements.

An explanation of how a safety requirement reduced the hazard's risk level—ultimately supported with objective evidence through testing, monitoring, or another method—must be provided for each safety requirement. All safety requirements that are implemented and are determined to have successfully addressed the hazard or safety issue become part of the operating NAS. At that time, they will be considered controls that form the basis for future SRM efforts. Refer to Section 3.7.2 for information on controls.

3.9.2.2 Risk Avoidance

The **risk avoidance strategy** averts the potential occurrence and/or consequence of a hazard by either selecting a different approach or not implementing a specific proposal. This technique may be pursued when multiple alternatives or options are available, such as determining where to construct an ATCT. In some cases, a decision may be made to limit the NAS change to certain conditions or system states, thereby avoiding the risk associated with other conditions. An example of this is allowing simultaneous operations on one runway that is overflown by three other runway flight paths. It may be discovered that the risk associated with the simultaneous operation can be mitigated to an acceptable level for two of the runways but not for the third. It may be decided that aircraft will not be allowed to operate on the third runway while simultaneously landing on the crossing runway, thereby avoiding risk.

A Comparative Safety Assessment (CSA) may be used when multiple systems or procedures are available.[14] If one alternative cannot be mitigated to an acceptable level, then another system, method, or procedure may be chosen. When no alternatives are available, the risk avoidance strategy is more likely to be used as the basis for a "go" or "no-go" decision at the start of an operation or program. Risk must be avoided from the perspective of all affected stakeholders. Thus, an avoidance strategy is one that involves all of the stakeholders associated with the proposed NAS change.

3.9.2.3 Risk Transfer

The **risk transfer strategy** shifts the ownership of risk to another party; the recipient may be better equipped to mitigate the risk at the operational or organizational level. Organizations transfer risk primarily to assign responsibility to the organization or operation most capable of managing it. The recipient must accept the risk, and the transfer must then be documented (e.g., through a Letter of Agreement or Memorandum of Agreement).

Examples of risk transfer may include:

- The transfer of aircraft separation responsibility in applying visual separation from the air traffic controller to the pilot,
- The development of new policies or procedures to change ownership of a NAS component to a more appropriate organization,

14. See the SRMGSA for more information on CSAs.

- The procurement of contracts for specialized tasks from more appropriate sources (e.g., contract maintenance), and
- The transfer of ATC systems from the acquisition organization to the organization that provides maintenance.

Risk transfer cannot be the only method used to treat a high-risk hazard. Identify safety requirements to lower the safety risk to medium or low before it can be accepted in the NAS. All transferred risks must be monitored until the predicted residual risk is verified by the appropriate organization.

3.9.2.4 Risk Assumption

The **risk assumption strategy** simply means accepting the risk. The risk acceptor assumes responsibility for the risk as it is. When a risk acceptor agrees to implement a NAS change, they agree to implement it based on the predicted residual risk being medium or low and assume responsibility for the risk. When this management strategy is used, the predicted residual risk is derived from the controls. Under this strategy, controls serve as the basis on which safety performance targets or alternate methods to verify predicted residual risk are developed. *It is recommended and desirable that safety requirements be developed to further mitigate risk or reduce likelihood or severity.*

It is not permissible to use a risk assumption strategy to treat an initial or current high risk associated with a hazard. The predicted residual risk for initial high-risk hazards must be medium or low before it can be accepted into the NAS.

3.9.3 Documenting Safety Requirements

All safety requirements identified by the SRM panel attendees and included in the HAW are considered to be recommendations for review and approval by the appropriate signatories. After appropriate means of managing risk have been developed and documented, management officials may identify the effect of safety requirements on other organizations and coordinate with the affected organizations.

If any safety requirement affects the safe provision of air traffic management services, it may be necessary for the safety requirement to undergo the SRM process to determine its effect on the NAS.

Refer to Section 5.3 for more information on safety requirements' approval and implementation decision-making and signatures.

3.9.4 Determining Predicted Residual Risk

Predicted residual risk is the risk that is estimated to exist after the safety requirements are implemented or after all avenues of risk mitigation have been explored. The predicted residual risk is based on the assumption that controls are in place and/or all safety requirements are implemented and are valid. If safety requirements are not documented in the HAW, predicted residual risk should be the same as the initial risk.

If the risk cannot be reduced to an acceptable level after attempting all possible risk reduction strategies, either revise the original objectives or abandon the proposed NAS change. If an acceptable proposal is not identified, the NAS change cannot be implemented. Similarly, if a NAS change was implemented without safety requirements and the predicted residual risk was not met, refer to Section 4.3.2 for more information.

4.1 Developing Safety Performance Targets

Safety performance targets[1] are measurable goals used to verify the predicted residual risk of a hazard. A safety performance target is the preferred means to relate the performance of risk reduction efforts to the expected risk level. The safety performance target is included as part of the monitoring plan (see Section 4.2).

Safety performance targets are used to assess safety performance with respect to controls and newly implemented safety requirements. Do not define the worst credible effect or effects producing the highest risk level as the safety performance target; instead, look at the less severe effects or indicators (e.g., the number of unauthorized vehicle deviations on taxiways per a specific number of airport operations over a period of time). Safety performance targets should be related to the hazard or National Airspace System (NAS) change.

When developing safety performance targets, the Safety Risk Management (SRM) panel attendees should apply the data used during the "Analyze Risk" phase of the DIAAT process to determine the appropriate metrics to monitor. (This DIAAT phase is described in Section 3.7.) If there is no established data source to support a proposed safety performance target, then a means to begin collecting the data should be identified and documented as a safety requirement. Data used during the SRM process also serve as the basis for comparison against the post-implementation metrics.

Mapping a hazard to a specific safety performance target may not be possible in terms of establishing a causal relationship. In such cases, identify a sound alternate method to verify the predicted residual risk and determine whether controls and/or safety requirements are appropriate and functioning as intended.

It is important to retain objective evidence that the safety requirements have been implemented. Objective evidence is simply documented proof. The evidence must not be circumstantial; it must be obtained through observation, measurement, testing, or other means.

4.2 Developing the Monitoring Plan

The monitoring plan[2] should be comprehensive enough to verify the predicted residual risk. The monitoring plan includes either the safety performance targets or another sound method for verifying the predicted residual risk. The SRM panel should create a plan for each hazard that defines:

- Monitoring activities;
- The frequency and duration of tracking monitoring results; and
- How to determine, measure, and analyze any adverse effects on adjoining systems.

4.2.1 Monitoring Activities

The risk acceptor, or the monitoring Point of Contact (POC) identified by the risk acceptor, must verify that the controls and/or safety requirements were implemented and are functioning as designed. Specifically, this means that procedures must be stringently followed and hardware or software must function within the established design limits.

1. Acquisition programs should refer to the Safety Risk Management Guidance for System Acquisitions (SRMGSA) for guidance on safety performance targets.

2. Segmented or phased acquisition programs should refer to the SRMGSA for guidance on monitoring.

Detail the methods by which the risk acceptor, or the monitoring POC identified by the risk acceptor, will gather the performance data and monitoring results. The organization that accepted the risk is accountable for ensuring that the monitoring plan is being upheld (i.e., that the monitoring results are being compared to the defined safety performance targets (or the results alone are being used) to determine whether predicted residual risk is being met). Refer to Section 5.4 for information about risk acceptance.

4.2.2 Frequency and Duration of Monitoring

When considering the frequency and duration of tracking monitoring results, account for:

- The complexity of the NAS change,
- The hazard's initial risk level,
- How often the hazard's effect is expected to occur in the defined system state (i.e., likelihood),
- Controls,
- The types of safety requirements that are being implemented (if any), and
- The amount of time needed to verify the predicted residual risk.

For example, when considering a hazard associated with the familiarity of a new procedure, a relatively short tracking period would be required until a person or population could reasonably be expected to adapt to the new procedure and the predicted residual risk could be verified. However, the monitoring plan for a hazard associated with new separation criteria may require several years of tracking to verify the predicted residual risk.

Refer to Annex A, Section 3.2.7, for documentation requirements of a complete monitoring plan for an individual hazard.

4.3 Post-SRM Monitoring

It is critical to obtain feedback on safety performance indicators through continuous monitoring. Organizations responsible for performing Quality Control and/or Quality Assurance use audits and assessments to monitor the safety risk and performance of an implemented NAS change documented in the monitoring plan. The responsible organization determines whether an implemented NAS change is meeting the safety performance targets documented in the monitoring plan.

Results of post-implementation monitoring help determine whether a change can be made part of the operating NAS or must be readdressed through the SRM process.

4.3.1 Monitoring and Current Risk

A hazard's current risk is updated at each monitoring interval (in accordance with stated monitoring frequency). Current risk provides an indicator of whether safety requirements are meeting the predicted residual risk. The risk acceptor is accountable for ensuring that the monitoring plan is being upheld and that monitoring reports, as dictated by the monitoring frequency, are being analyzed to determine whether the safety performance targets are being met.

4.3.2 Predicted Residual Risk Is Not Met

Through monitoring current risk and the safety performance of a recently implemented NAS change, it may become clear that the predicted residual risk is not being met. If this occurs, notify the risk acceptor. The risk acceptor may choose to accept the current risk as the new predicted residual risk or to reconvene the SRM panel for additional safety requirement considerations. In either case, the SRM document must be revised with the new safety requirements (if identified) and new predicted residual risk, and approval and risk acceptance signatures must be reobtained (refer to Section 5.4.1 for information on risk acceptance authority).

There are several reasons why the predicted residual risk may not be met:

- The safety requirements or controls may not be properly mitigating the risk,
- The initial risk may have been analyzed inaccurately,
- Unintended consequences may have occurred, or
- New hazards may have been identified.

Refer to Section 5.7 for information on updating SRM documentation.

4.3.3 Predicted Residual Risk Is Met

The successful completion of monitoring is a prerequisite to hazard and NAS change closeout. This includes the achievement of safety performance targets and/or the predicted residual risk.

The monitoring procedures used to verify the predicted residual risk must also be documented, as they will be used to evaluate the safety performance of the change after it is added to the operating NAS. The established monitoring requirements must be followed, even after meeting the goals of the monitoring plan.

4.3.4 Residual Risk

Residual risk is the level of risk that has been verified by completing a thorough monitoring plan with an achieved measurable safety performance target(s). It is the composite of the severity of a hazard’s effect and the frequency of the effect’s occurrence.

4.3.5 Monitoring and Tracking of Changes Added to the Operating NAS

A change is considered part of the operating NAS only after monitoring through existing Safety Assurance processes is completed, the safety performance target is achieved and maintained, and/or the predicted residual risk is verified. The NAS change and all the associated safety requirements become part of the operating NAS, which will become the basis from which all future NAS changes will be measured. If a safety requirement is altered or removed from a NAS change that was made part of the operating NAS, SRM must be performed.

The documentation that was developed during the SRM process is critical to Safety Assurance functions, which often use SRM documents as inputs to assessments and evaluations.

5.1 Risk Acceptance and Approval

The review and approval of Safety Risk Management (SRM) documents and acceptance of any safety risk is designed to maintain and assure the quality of Air Traffic Organization (ATO) safety risk management activities. There are key variables that affect safety risk acceptance and SRM documentation review and signature requirements. They include the organization(s) affected by the proposed National Airspace System (NAS) change, the organization that developed the document, the safety risk(s) associated with the NAS change, and whether the NAS change is considered national or local in scope. There are several signature authorities associated with SRM documentation: concurrence, approval, risk acceptance, and safety requirement implementation. Refer to Section 5.2 for information regarding changes that are nationally and locally scoped.

For guidance on specific signature types, refer to Sections 5.3 through 5.6. Tables 5.1 through 5.4 summarize SRM document signature requirements. The terms "affected facilities" and "affected Service Units" refer to the facilities or organizations that are impacted by the safety risk associated with the NAS change or existing safety issue.

Note: Table 5.1 is not to be used for SRM documents with an unacceptable (high) predicted residual risk (see Table 5.4).

Table 5.1: Approval and Risk Acceptance Signatures for SRM Documents With Hazards (Use with Annex A, Section 3) (1) (2) (14) (15)

<table>
<tr><th>Type of Change</th><th>Requires AOV Approval/Acceptance? (3)</th><th>Initial Predicted Risk Level</th><th>Required SRM Document Approval Signatures (4)</th><th>Required Safety Risk Acceptance Signatures (16)</th></tr>
<tr><td rowspan="3">Local</td><td>No</td><td>Low/Medium (5)</td><td>Support Managers or System Support Center Managers of the affected facilities (6)</td><td>Air Traffic Managers or Technical Operations Managers of the affected facilities</td></tr>
<tr><td rowspan="2">Yes</td><td>Low/Medium (5)</td><td>Support Managers (6) or System Support Center Managers, AJI-3 Director (8) (9)</td><td>Air Traffic Managers or Technical Operations Managers of the affected facilities</td></tr>
<tr><td>High (7)</td><td>Headquarters Director(s) or Technical Operations Service Area Director, AJI-3 Director (8)</td><td>Vice President of the affected Service Unit</td></tr>
<tr><td rowspan="2">National</td><td rowspan="2">Yes/No</td><td>Low/Medium (5)</td><td>Headquarters Group Manager of the change proponent, AJI-3 Director (8)</td><td>Headquarters Director(s) of the affected Service Unit(s)</td></tr>
<tr><td>High (7)</td><td>Headquarters Director(s) of the affected Service Unit(s),
AJI-3 Director (8)</td><td>Vice President(s) of the affected Service Unit(s)</td></tr>
</table>

Type of Change	Requires AOV Approval/Acceptance? (3)	Initial Predicted Risk Level	Required SRM Document Approval Signatures (4)	Required Safety Risk Acceptance Signatures (16)
Acquisitions (10)	Yes/No	Low/Medium (5)	Director of Mission Support Services Strategy, Director of Program Management Organization, AJI-3 Director (11) (12)	Headquarters Director(s) of the affected Service Unit(s) (13)
		High (7)	Director of Mission Support Services Strategy, Director of Program Management Organization, AJI-3 Director (11) (12)	Vice President(s) of the affected Service Unit(s) (13)

Notes:

(1) The change proponent must ensure that the SRM document is entered into the Safety Management Tracking System (SMTS) for tracking and monitoring the status of the NAS change / existing safety issue.

(2) Signature responsibility may only be delegated from a Director to a Deputy Director.

(3) The changes that require Air Traffic Safety Oversight Service (AOV) approval are listed in Federal Aviation Administration (FAA) Order 1100.161, *Air Traffic Safety Oversight*. If there is an initially identified high-risk hazard, AOV must approve the means to reduce safety risk and the Service Area Director of Operations or Technical Operations Service Area Director and the Director of Safety (AJI) Policy and Performance, AJI-3, (8) must sign the document.

(4) If the AJI-3 Director's approval is required, then the proponent of an air traffic change / existing safety issue must send a copy of the SRM document to the Director of Air Traffic Operations (Service Area) for informational purposes only before submitting the SRM document to the AJI-3 Director.

(5) In cases where medium or low safety risk and/or controls go outside of the ATO, the mitigations must be approved by the designated management officials within the other Lines of Business (LOBs) and accepted by AOV.

(6) If a facility does not have a Support Manager, the Assistant General Manager or General Manager of the affected facility shall designate an SRM document approver.

(7) The AJI-3 Director must submit safety cases with means to reduce safety risk of any initially identified high-risk safety hazards to AOV for approval.

(8) If the change or existing safety issue meets the criteria for AOV approval, the AJI-3 Director must submit it to AOV accordingly.

(9) SRM documents that accompany air traffic waiver requests must also be signed by the Service Area Director of Air Traffic Operations.

(10) See the Safety Risk Management Guidance for System Acquisitions (SRMGSA) for details on which safety deliverables must be approved by the AJI-3 Director or by the Program Management Organization (AJM).

(11) Some safety documentation developed for acquisition programs must undergo a peer review before signature, as described in the SRMGSA. Refer to Section 8 of the SRMGSA for more information.

(12) The Director of Mission Support Services (AJV) Strategy, AJV-S, or their designee must provide their approval when the safety requirements are not already documented in an approved Program Requirements Document (PRD).

(13) Risk acceptance must be obtained for SRM documents in which risk is identified, except for the Operational Safety Assessment and the Comparative Safety Assessment.

(14) For approval and/or risk acceptance outside of the ATO, AOV may facilitate signatures on behalf of the ATO. However, the Service Unit change proponent should obtain signatures from the affected organization (user) participating on the SRM panel.

(15) Second-Level Engineering should start with Table 5.2 for their signature requirements.

(16) FAA Contract Towers (FCTs) can concur with but cannot accept risk into the NAS. The General Manager or Assistant General Manager accepts risk on the behalf of the FCT.

Table 5.2: Approval and Risk Acceptance Signatures for Second-Level Engineering SRM Document (1) (2) (3)

<table>
<tr><th>Proposed Modification to Approved System-Level Requirements? (4)</th><th>Previous SRM Document Identifying Safety Implications of the Proposed Modification?</th><th>Facilitated by AJI or Requires AOV Approval or Acceptance? (5) (6) (7)</th><th>Hazard(s) Identified?</th><th>Required SRM Document Approval Signatures</th><th>Required Safety Risk Acceptance Signatures</th></tr>
<tr><td rowspan="5">No</td><td>Yes</td><td colspan="4">No additional SRM required</td></tr>
<tr><td rowspan="4">No</td><td rowspan="2">No</td><td>Yes</td><td>Headquarters Group Manager of the change proponent</td><td>Headquarters Director(s) of the affected Service Unit(s)</td></tr>
<tr><td>No</td><td>Headquarters Group Manager of the change proponent</td><td>None</td></tr>
<tr><td rowspan="2">Yes</td><td>Yes</td><td colspan="2">See signature requirements in Table 5.1</td></tr>
<tr><td>No</td><td>Headquarters Group Manager of the change proponent, AJI-3 Director</td><td>None</td></tr>
<tr><td rowspan="4">Yes</td><td rowspan="4">Yes/No</td><td rowspan="2">Yes</td><td>Yes</td><td colspan="2">See signature requirements in Table 5.1</td></tr>
<tr><td>No</td><td>Headquarters Group Manager of the change proponent, AJI-3 Director</td><td>None</td></tr>
<tr><td rowspan="2">No</td><td>Yes</td><td colspan="2">See signature requirements in Table 5.1</td></tr>
<tr><td>No</td><td>Headquarters Group Manager of the change proponent, AJI-3 Director</td><td>None</td></tr>
</table>

Notes:

(1) This table applies to national-level NAS changes only. For local changes, refer to Table 5.1.

(2) The change proponent must ensure that the SRM document is entered into SMTS for tracking and monitoring the status of the NAS change / existing safety issue.

(3) Signature responsibility may only be delegated from a Director to a Deputy Director.

(4) System Level Requirements refer to the requirements listed in the Final PRD.

(5) The changes that require AOV approval are listed in FAA Order 1100.161.

(6) In cases where medium or low safety risk and/or controls go outside of the ATO, the means to reduce safety risk must be approved by the designated management officials within the other LOBs and accepted by AOV.

(7) The AJI-3 Director must submit the means to reduce safety risk of any initially identified high-risk safety hazards to AOV for approval.

Table 5.3: Approval Signatures for SRM Safety Decisions and SRM Documents Without Hazards (Use with Annex A, Section 3) (1) (2) (4)

Type of Change	Required SRM Document Approval Signatures
Local (3)	Director of Air Traffic Operations (Service Area); Assistant General Manager or General Manager; or Technical Operations Manager or Assistant General Manager
National	Headquarters Director(s) of affected Service Unit(s), AJI-3 Director
Acquisitions (5)	Headquarters Director(s) of affected Service Unit(s), AJI-3 Director

Notes:

(1) The documentation to which this table applies includes SRM Safety Decisions and SRM Documents Without Hazards. The change proponent must ensure that the SRM documentation is entered into SMTS for tracking and monitoring the status of NAS changes.

(2) Signature responsibility may only be delegated from a Director to a Deputy Director.

(3) For local changes, the SRM documentation is signed one level above the Air Traffic Manager at the facility completing the SRM documentation.

(4) This table does not apply to Second-Level Engineering.

(5) See the SRMGSA for details on which safety deliverables must be approved by the AJI-3 Director or by AJM.

Table 5.4: Approval Signatures Only for SRM Documents for Proposed NAS Changes (Use with Unacceptable (High) Predicted Residual Risk) (1) (2) (3)

Type of Change	Required SRM Document Approval Signatures
Local (4)	Air Traffic Managers or Technical Operations Managers of the affected facilities
National	Headquarters Director(s) of the affected Service Unit(s), AJI-3 Director

Notes:

(1) When the predicted residual risk is unacceptable (high), the proposed NAS change cannot be implemented; therefore, AOV approval is not required.

(2) Per ATO Safety Management System (SMS) policy, a high predicted residual risk is unacceptable and the NAS change in question must not be implemented. The SMTS submitter is responsible for notating this in SMTS and closing out the project. (See the SMTS User Manual.)

(3) Signature responsibility may only be delegated from a Director to a Deputy Director.

(4) For local changes, the SRM document is signed one level above the Air Traffic Manager at the facility completing the SRM document.

5.2 Scope of NAS Changes

NAS changes are considered either local or national. A national NAS change is one for which an AJI Safety Case Lead (SCL) facilitates or leads the SRM effort or that meets at least one of the following criteria:

- The NAS change has high visibility or a potential political, economic, or financial impact on the FAA, the NAS, or the flying public.[1]
- The NAS change is the result of financial or operational decisions made by FAA executive management, Cabinet-level executives, or Congress.
- The NAS change includes means to reduce any safety risk identified as a high-priority safety issue by AJI.
- The NAS change modifies safety policy that must be incorporated into a directive.
- The NAS change could or does present operational or technical conflicts to multiple affected Service Units or FAA LOBs.
- The NAS change will be implemented on a national level, affecting multiple facilities.

Note: There may be cases in which an AJI SCL facilitates a local SRM panel and none of the aforementioned criteria apply. These changes will be considered local.

A NAS change is considered to be local if:

- It does not meet any of the preceding criteria and it affects three or fewer Service Delivery Points within a single Service Area, or
- It is a change proposed by Technical Operations that involves a single piece of equipment that is restricted to one district.

In cases where a NAS change affects two adjacent Service Delivery Points in different Service Areas or a single Terminal Radar Approach Control / Air Route Traffic Control Center with more than two underlying Airport Traffic Control Towers, the change proponent has the authority to determine if the change will be considered local or national in scope.

Note: Many systems and facilities that provide service in the NAS are not procured, owned, or maintained by the FAA or another federal entity. The FAA has the authority and responsibility to

1. AJI will typically identify these types of changes.

assure the safety of these services in accordance with Title 49 of the United States Code Section 44505, *Systems, procedures, facilities, and devices*, and Title 14 of the Code of Federal Regulations Part 171, NON-FEDERAL NAVIGATION FACILITIES. Although a system/service may not be procured by the FAA, implementation into the NAS is considered a NAS change and requires appropriate SRM as if the FAA were acquiring the system/service.

5.2.1 Local Implementation of National NAS Changes

When the local implementation of a nationally scoped SRM document cannot follow the national standard, local SRM is required for the local deviations. If formal waivers are required in such cases, local SRM does not eliminate the waiver requirement.

5.3 Approving Safety Requirements

An organization's safety requirement approval signature represents its commitment to implementing the safety requirement in accordance with the associated SRM document. For acquisition systems, if the approved PRD contains the safety requirements referenced in the SRM document, no Point of Contact (POC) signature is required. If the requirements are not listed in the approved PRD, the SRM document must include a POC signature for each additional safety requirement.

5.3.1 Appropriate Signatories

Safety requirement signature authority must be at the managerial level with the ability to fund and ensure the implementation of the safety requirement. The appropriate signing official may be determined by the FAA organization. When multiple officials are responsible for providing safety requirements signatures for an SRM document, they must share similar managerial statuses or responsibilities.

When an organization outside of the FAA is responsible for a safety requirement, a signature on file is required. This requirement may be met through a memorandum or an SRM document. The change proponent is responsible for following up on the status of the implementation of safety requirements identified in the SRM document.

5.3.2 Endorsing Implementation of Safety Requirements

All safety requirements that the SRM panel attendees identify must be accounted for in the SRM document. The change proponent and appropriate safety requirement(s) POC(s) must collaborate to determine which safety requirements will be approved for implementation and notate that decision in the SRM document. The risk acceptor is accountable for ensuring that all approved safety requirements are implemented and all monitoring activities are recorded in SMTS.

5.3.2.1 Safety Requirements Planned for Implementation

All safety requirements included in the Hazard Analysis Worksheet (HAW) of the signed SRM document must be implemented before or in conjunction with the NAS change, even when the risk is classified as medium or low. All organizations responsible for implementing a safety requirement must:

1. Sign the SRM document for the safety requirement approval,
2. Document the status of the safety requirement (e.g., implemented, not implemented, or in progress), and

3. Record objective evidence supporting the safety requirement's implementation.

Only safety requirements that are to be implemented must have an accompanying signature.[2]

5.3.2.2 Safety Requirements Not Planned for Implementation

If a safety requirement is not going to be implemented, SRM panel attendees must be contacted to verify that the predicted residual risk, safety performance target(s), and/or monitoring plan have not been affected. If changes are required, the SRM panel attendees must reconvene to update any impacted section of the SRM document, including the HAW,[3] and the SRM document must be revised to include these changes and the rationale for not implementing the safety requirement. In addition, if any of the SRM panel members dissent with the removal of the safety requirement or the resulting changes to the predicted residual risk, safety performance target(s), and/or monitoring plan, the dissention must be included in the SRM document.

5.3.3 Safety Recommendations

Safety recommendations do not rise to the level of safety requirements. They are not used when determining predicted residual risk and do not require any endorsement but may be recorded within the SRM document.

5.4 Risk Acceptance

Risk acceptance is confirmation by the appropriate management official that they understand the safety risk associated with the NAS change or existing safety issue and that they accept that safety risk into the NAS. Safety risk must be accepted before the implementation of a proposed NAS change and the execution of the monitoring plan. Risk acceptance is based on the predicted residual risk. Risk acceptance and other inputs (e.g., cost-benefit analysis) are necessary before a change to the NAS can be implemented. When an individual or organization accepts a risk, it does not mean that the risk is eliminated; some level of risk will remain.

Risk acceptance requires:

- Signed confirmation from the appropriate management official that they understand and accept the predicted residual safety risk(s) associated with the hazard(s) identified in the SRM document;
- Signatures for the safety requirements identified in the SRM document;
- Approval of the safety performance target(s) or alternate method(s) identified to verify the predicted residual risk associated with each hazard, confirming that the safety performance target(s) or identified alternate method(s) can be used to measure the current risk; and
- A comprehensive monitoring plan that the risk acceptor agrees to follow to verify the predicted residual risk.

For nationally implemented NAS changes, risk can be accepted at the national level. However, if a facility is not able to comply with all of the safety requirements or has additional hazards and/or causes that were not identified in the national SRM document, the facility must perform

2. A PRD may be used in lieu of providing signatures for safety requirements; see the SRMGSA for more information.

3. This reconvene can be conducted in person or via telephone or video conference.

SRM (with local risk acceptance) prior to the implementation of the NAS change. Refer to Section 5.2.1 for information on local versus national implementation of safety requirements.

5.4.1 Authority to Accept Safety Risk

The acceptance of the safety risk depends on the span of the program or NAS change and the associated risk. The responsibility for risk acceptance ultimately lies with the organization(s) affected by the NAS change. Risk acceptance authority also depends on whether a NAS change is local or national in scope.

By signing the SRM document, the risk acceptor is confirming the following are understood and accepted:

- The identified safety risk(s);
- The safety requirements that will be implemented;
- The predicted residual risk(s) associated with the hazard(s);
- The safety performance target(s) identified to measure the predicted residual risk associated with each hazard, thus confirming that the safety performance target(s) may be used to measure the current risk level; and
- The information contained in the monitoring plan.

The risk acceptor is accountable for:

- Ensuring that all monitoring activities are being recorded in SMTS;
- Ensuring that performance data needed for the monitoring activities are being collected and analyzed to verify that the safety performance target(s) are being met;
- Determining the need to reconvene SRM panel attendees[4] or choosing to accept the current risk as the new predicted residual risk if performance data indicate that the predicted residual risk is not met and/or if the risk management strategy is proven to be inadequate; and
- Reconvening the SRM panel attendees if a safety requirement identified by the attendees cannot be implemented.

5.4.2 Risk Acceptance Outside of the ATO

If the affected party is outside of the ATO (e.g., navigation or weather services), each organization responsible for establishing requirements for contracted services accepts the risk into the NAS. LOBs/organizations outside of the ATO (e.g., Office of Airports, Office of NextGen, Office of Commercial Space Transportation, or Office of Aviation Safety) are also responsible for components of the NAS and have a role in accepting safety risk. Organizations or individuals external to the ATO cannot, however, accept risk on the ATO's behalf. (An FCT may act as a change proponent, but it may not accept safety risk.)

ATO vice presidents, directors, managers, and supervisors must work closely with their counterparts in LOBs/organizations outside of the ATO to help ensure that the appropriate party or parties accept and manage any safety risk resulting from NAS changes. (See Section 3.9.2.3 for more information on risk transfer strategy.) Again, it is not in compliance with ATO policy to

4. This reconvene can be conducted in person or via telephone or video conference.

implement a NAS change without having first accepted any associated safety risk. Refer to FAA Order 8040.4, *Safety Risk Management Policy*, for policy on cross-LOB risk acceptance.

5.5 SRM Documentation Concurrence

Concurrence is used to represent a technical review of the SRM document and to confirm the rationale used throughout is consistent with the SRM process. The concurrence signature comes from an SRM expert who is well versed in the ATO SMS Manual and familiar with the terminology and processes therein. The concurrence signature is not a required signature; however, Service Areas, District Offices, or individual facilities may require a concurrence signature on their respective SRM documentation.

5.6 SRM Documentation Approval

Approval of an SRM document with hazards requires and represents that:

- The SRM document was developed in accordance with policy and guidance;
- Hazards were systematically identified using a structured approach;
- Risk was appropriately analyzed and assessed;
- If identified, safety requirements were deemed valid;
- Safety performance targets or other methods to verify predicted residual risk were approved by the responsible Service Unit; and
- A monitoring plan was prepared.

Approval of an SRM document without hazards requires and represents that:

- The SRM document was developed in accordance with policy and guidance,
- The NAS change did not introduce new hazards or increase safety risk, and
- The SRM document includes a detailed rationale to support the finding of no hazards.

In approving SRM documentation, the approval authority affirms that the aforementioned items have been performed and agrees that the underlying assumptions are reasonable and the findings are complete and accurate. SRM documentation approval does not constitute approval for implementation or acceptance of any risk associated with the NAS change or existing safety issue.

Approval of an SRM Safety Decision requires and represents that a manager at the district or equivalent level (or above) is aware of the SRM activity, its results (i.e., the results of the Preliminary Safety Assessment), and any other safety-related findings/information related to the proposed change (e.g., full system description or Two-Phase Local SRM findings).

5.6.1 Service Unit SRM Documentation Approval or Concurrence

Affected or stakeholder Service Units must assign an appropriate management official to provide approval or concurrence (when applicable) of SRM documentation. The person selected must be available to provide input to the management official(s) who will accept the risk associated with the NAS change or existing safety issue.

If SRM documentation must be sent outside of the Service Unit for approval (to another Service Unit, another LOB, AJI, or AOV), the documentation must have an approval or concurrence signature before it leaves the Service Unit. All identified means to reduce safety risk requiring approval and acceptance by AOV must first be sent through AJI.

If SRM documentation requires the approval or concurrence of more than one Service Unit, discrepancies in the approval standards or processes may exist between the organizations. In these cases, the change proponent should request that AJI adjudicate the discrepancies.

If an AJI SCL managed the development of the SRM documentation (see Annex A), no other Service Unit concurrence is required; however, the risk acceptor must still review and sign the SRM document before the NAS change can be implemented. If an AJI SCL develops the SRM document, the relevant/affected operational Service Unit(s) that accepted the associated risks of the NAS change or existing safety issue must follow the monitoring plan documented in the SRM document.

5.6.2 AJI Review and Approval

AJI SCLs verify that the SRM process has been followed, that the safety documentation is complete, and that the safety documentation adheres to the SMS Manual principles and guidelines. Any documentation forwarded to the AJI-3 Director for approval must first go through an AJI peer review.[5] To submit SRM documentation for AJI peer review, send it in draft form, without signatures, to the AJI-314 Safety Engineering Team Manager via the AJI Safety Engineering Team mailbox. The AJI-314 Manager will assign an AJI SCL to coordinate the peer review process. At this point, the AJI SCL will facilitate the remaining steps in the review process. When the SRM document is ready for signature, the AJI SCL will notify the change proponent, who will obtain the appropriate signatures. Finally, when the SRM document has all signatures except for that of the AJI-3 Director, the AJI SCL will present the SRM document to the Safety Management Group, AJI-31, Manager. The AJI-31 Group Manager will forward the SRM document to the AJI-3 Director for signature. Other SRM document signature requirements that are documented in this SMS Manual remain.

When a NAS change or existing safety issue facilitated by AJI crosses FAA LOBs/organizations, an AJI SCL reviews the SRM document to verify that affected LOBs/organizations have reviewed and approved the documentation. In addition, the AJI-3 Director must approve and sign it.

5.6.2.1 AJI Participation in System Acquisition SRM

AJI SCLs will be involved with NAS change efforts from concept development through In-Service Management. An AJI SCL will be assigned to a portfolio or program to provide safety guidance and advice, as appropriate. The AJI SCL will be familiar with the portfolio or program, its possible interfaces, its position within the Enterprise Architecture, its milestones, and its safety documentation requirements. The AJI SCL will stay with that portfolio or program throughout its lifecycle.

The AJI SCL will ensure that all required safety documentation meets the requirements of this SMS Manual and the SRMGSA and will request subject matter experts to review (i.e., peer review) certain documentation before it is presented to the AJI-3 Director for approval.

5. Peer reviewers objectively review the document to ensure the analysis/assessment is accurate and operationally sound (i.e., the safety hazards, causes, effects, and safety requirements are appropriate).

The AJI-3 Director reviews certain SRM documentation and the associated acquisition safety assessments, analyses, reports, and plans, providing approval or comments (see the SRMGSA for information regarding specific documentation reviews and approval requirements).

5.6.3 AOV Approval and Acceptance

5.6.3.1 Items Requiring AOV Approval

AOV approval is the formal act of approving a NAS change submitted by a requesting organization. This action is required prior to the proposed NAS change being implemented. This is not the same as approval of the SRM document itself. All NAS changes or existing safety issues submitted to AOV for approval first require approval and concurrence by AJI and any applicable Service Units. Refer to Section 5.6.2 for information on AJI approval.

The following items require AOV approval before implementation:

- Controls that are defined to mitigate or eliminate initial and current high-risk hazards. (For specific guidance regarding the AOV high-risk hazard acceptance/approval process and modeling requirements, see FAA Order 1100.161; AOV *Safety Oversight Circular (SOC) 07-02, AOV Concurrence/Approval at Various Phases of Safety Risk Management Documentation and Mitigations for Initial High-Risk Hazards*; and AOV SOC 07-05A, *Guidance on Safety Risk Modeling and Simulation of Hazards and Mitigations*.)
- Changes, waivers, or authorizations (when prescribed in an ATO directive) to provisions of handbooks, orders, and documents that pertain to separation standards, including FAA Order JO 7110.65, *Air Traffic Control*
- Changes to NAS equipment availability and any changes to the program
- Changes to the ATO SMS Manual; the SRMGSA; FAA Order JO 1030.1, *Air Traffic Organization Safety Guidance*; FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*; or any other ATO-initiated orders, notices, or ATO Safety Guidance affecting the ATO SMS

5.6.3.2 Items Requiring AOV Acceptance

The following require acceptance by AOV:

- Mitigations to reduce high safety risk to medium or low and/or mitigations that cross FAA LOBs
- Exclusions to SMS requirements granted by AJI
- Changes to the criteria in FAA Order 8200.1, *United States Standard Flight Inspection Manual*, including:
    - The flight inspector's authority and responsibilities
    - Facility status classification and issuance of a Notice to Airmen (NOTAM)
    - Records and reports
    - Extensions in the periodicity or interval of inspections
    - Changes in required checklist items for the inspection of specific system areas

  - Changes in established tolerances, or tolerances proposed for new equipment or new functionality
  - Changes in the procedures for evaluating the safety and flyability of instrument flight procedures

- Changes to the personnel certification requirements
- Changes to the certification criteria in FAA Order 6000.15, *General Maintenance Handbook for National Airspace System (NAS) Facilities*
- Changes to the personnel certification requirements in FAA Order JO 3000.57, *Air Traffic Organization Technical Operations Training and Personnel Certification*
- Changes to the Aeronautical Information Services (AIS) Credentialing Standard Operating Procedure
- Corrective Action Plans that AOV requires

5.6.4 Coordination of SRM Documentation

AJI will collaborate with AOV to obtain the necessary reviews, approval, and risk acceptance signatures for SRM documentation with all applicable organizations outside of the ATO for all NAS changes. The scope of potential changes includes products, services, systems, and procedures associated with federal and non-federal facilities. Service Unit change proponents may initiate these reviews and signatures through outside ATO organizations. However, the Service Unit change proponent must inform the appropriate AJI SCL of such action.

5.7 Revising an SRM Document

Through post-implementation monitoring, a need to modify the previously approved SRM document may arise (see Section 4.3.2). This requires a revision of the SRM document and new SRM document approval and risk acceptance signatures.

Table 5.5: Signature Requirements for Revisions of SRM Documents (1)

Part of SRM Document Changed	Type of Change	Version Protocol	New SRM Document Approval Signature and Risk Acceptance Required?
System description	Updating charts, maps, airport layout, and approach plates, as long as change does not affect hazards or risk levels	Decimal revisions (e.g., 1.0 to 1.1, 1.2)	No
HAW	New hazard; change to predicted residual risk	Whole number revisions (e.g., 1.0 to 2.0)	Yes
HAW to include safety requirements	Adding, changing, removing, or not implementing new or existing safety requirements	Whole number revisions	Yes
Hazard and risk analysis	Adding rationale or data for risk analysis when risk is not changed and/or means to reduce safety risk are not added or changed	Decimal revisions	No

Part of SRM Document Changed	Type of Change	Version Protocol	New SRM Document Approval Signature and Risk Acceptance Required?
Safety requirements, monitoring plan, and appendices	Clarification of safety requirements, including Standard Operating Procedures, Letters of Agreement, letters to airmen, and implementation and monitoring reports, as long as risk is not changed and means to reduce safety risk are not added or changed	Decimal revisions	No

Notes:

(1) If an SRM document revision does not necessitate a new approval/acceptance signature from AOV, a new signature from the AJI-3 Director is not required.

The risk acceptor(s), in coordination with the change proponent, may need to update or change an SRM document as a project progresses and decisions are modified. Monitoring may indicate that the NAS change does not meet the predicted residual risk, that the risk management strategy is less effective than expected, or that additional hazards exist. In this case, additional safety requirements may be necessary. Any change that may affect the assumptions, hazards, causes, or estimated risk in an SRM document necessitates a revision, including new signatures. A change page (containing a description of each change to the SRM document and the number of each affected page) must be included with each SRM document.

Based on the results of external assessments (e.g., Independent Operational Assessments, Flight Inspections, post-implementation safety assessments, AJI audits and assessments, and the NAS Technical Evaluation Program), the change proponent may need to reconvene the SRM panel attendees and update the SRM document as needed.

6.1 Audit and Assessment Programs

Safety (AJI) Safety Assurance programs evaluate compliance with Safety Management System (SMS) requirements and Federal Aviation Administration (FAA) and/or Air Traffic Organization (ATO) orders, standards, policies, and directives. Findings from these assessments could require that the change proponent reconvene the Safety Risk Management (SRM) panel attendees and update the SRM document as needed.

Audit and assessment programs evaluate:

- The effectiveness of each Service Unit's performance and operations;
- The effectiveness of Air Traffic Control (ATC) facilities' and Technical Operations (AJW) Districts' internal Quality Control efforts (e.g., operational skills assessments, system service reviews, certification, periodic maintenance, data integrity, modification, and availability);
- The effectiveness of Quality Control mitigation efforts in response to identified trends and risks;
- Trends identified from safety data analysis;
- The effectiveness of safety-related policies and procedures; and
- Compliance with and maturity of the ATO's SMS.

6.1.1 ATO Compliance Verification Evaluation Program

FAA Order JO 7210.633, *Air Traffic Organization (ATO) Quality Assurance (QA)*, and FAA Order JO 7210.634, *Air Traffic Organization (ATO) Quality Control*, describe the current ATC facility evaluation and assessment programs that involve assessments and audits focusing on compliance and safety. Air Traffic Service Area Directors, Air Traffic Managers and AJW Districts are responsible for conducting internal evaluations of their respective facilities. The Safety Services Group, AJI-15, retains oversight of the ATC evaluation process and performs program assessments.

6.1.2 Difference between ATC Facility Audits and Assessments

The Air Traffic Manager conducts internal compliance verifications of their facility in accordance with FAA Order JO 7210.634. AJI conducts audits based on identified or suspected safety issues and noncompliance in accordance with FAA Order JO 1000.37, *Air Traffic Organization Safety Management System*. The office determines priorities by soliciting input from the Service Areas and other FAA Lines of Business (LOBs) and by analyzing objective criteria from sources such as occurrence reports and risk analysis results. In addition, AJI conducts no-notice spot inspections of ATC facilities and AJW activities, including the Aviation System Standards group.

6.1.3 National Airspace System Technical Evaluation Program

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

The NAS Technical Evaluation Program provides AJI with asset management and safety decision-making information based on an independent review of:

- How well facilities and services meet their intended objectives:
    - Evaluators check key performance parameters and certification parameters at selected facilities.
    - Evaluators review NAS Performance Analysis and NAS Performance Index data.
- How well the maintenance program is executed:
    - Evaluators review facility logs to verify certification, periodic maintenance accomplishments, and documentation of corrective and scheduled maintenance activities.
    - Evaluators review the completion of required modifications.
    - Evaluators review facility documentation, such as Technical Performance Records, and required reference data.
- How well customer needs are being met:
    - Evaluators solicit customer feedback through interviews and surveys.
    - Evaluators review the outage coordination process.

Evaluators may also review specialist certification records and credentials. These reviews are either part of a special inspection or are random spot checks of documentation in a location that is geographically convenient to the routine evaluation.

6.1.4 Independent Operational Assessments

AJI supports the agency's commitment to field-safe and operationally ready solutions by conducting Independent Operational Assessments (IOAs) on designated new or modified systems or capabilities before the In-Service Management phase. An IOA is a full system- or capability-level evaluation conducted in an operational environment. An IOA's purpose is to confirm the readiness of a system from an operational and safety perspective. IOAs are independent of the Program Management Organization (AJM) implementing the solution. IOAs evaluate systems against pre-determined critical operational issues. Hazards identified by an IOA must still undergo all necessary phases of the SRM process by the change proponent.

The Vice President of AJI directs the commencement of an IOA after the acceptance of an IOA Readiness Declaration from the Vice President of AJM. To assess the system/capability, AJI collaborates with the organizations that will operate, maintain, or otherwise be operationally affected by the solution. AJI reports any new or previously identified hazards, as well as operational concerns, based on data observed and collected during the IOA.

At the conclusion of an IOA, the team assesses the solution's operational readiness based on the identified hazards and any observed operational concerns. The team reports and briefs the results of the IOA to affected stakeholders, including the Vice President of AJI, AJM, the affected operating service(s), and any other affected organizations. The results are also provided to the In-Service Decision authority. The change proponent is responsible for the treatment and monitoring phases of SRM for the hazards identified during the IOA.

6.1.5 Independent Assessments

AJI performs independent assessments to evaluate operational procedures, order compliance, fielded systems, and safety benefits. An AJI independent assessment is independent of the Program Office or operating service responsible for the program or operation. They are post-implementation evaluations of NAS changes that assess actual performance.

During independent assessments, the teams verify that any previously documented hazards were rated accurately (based on observed data) and that no unacceptable safety risks exist. In addition, teams may identify operational issues and other findings.

Independent assessments may involve several facility or program assessments over a long period of time, one assessment that lasts for an extended period of time, or multiple brief assessments. The processes and procedures are tailored according to the duration of the assessment and the complexity of the operation or program being assessed. The assessment may be conducted at one or multiple sites, and data may be collected on site or remotely. Results and/or recommendations are based on the assessment team's analysis of data collected during and, if applicable, before the assessment. The conclusions and recommendations are independent from external sources.

6.2 Safety Data Reporting, Tracking, and Analysis

SMSs require the collection and analysis of data from different sources and various vantage points to determine if hazards exist. An important aspect of safety data analysis is developing the capability to sort and analyze a vast array of data and transforming that data into information that permits the identification and mitigation of hazards, thus preventing future incidents and accidents.

6.2.1 Purpose of Safety Data Collection and Evaluation

The tracking and analyzing of safety data to enhance the ATO's awareness of potentially hazardous situations is a critical aspect of the SMS. AJI assists with the collection and analysis of agency-wide safety data and supports sharing the data to continually improve the safety of the NAS.

Safety data are used to:

- Identify risks, systemic trends, and vulnerabilities in the system;
- Determine the effects of a NAS change on the operation as a whole;
- Assess the performance of safety requirements in managing risk;
- Identify areas where safety could be improved;
- Contribute to accident and incident prevention; and
- Assess the effectiveness of training.

In most cases, if the analysis of safety data leads to the identification of issues or hazards, the resolution or corrective action constitutes a NAS change, which requires SRM. This is an example of the continuous, closed-loop process for managing safety risk.

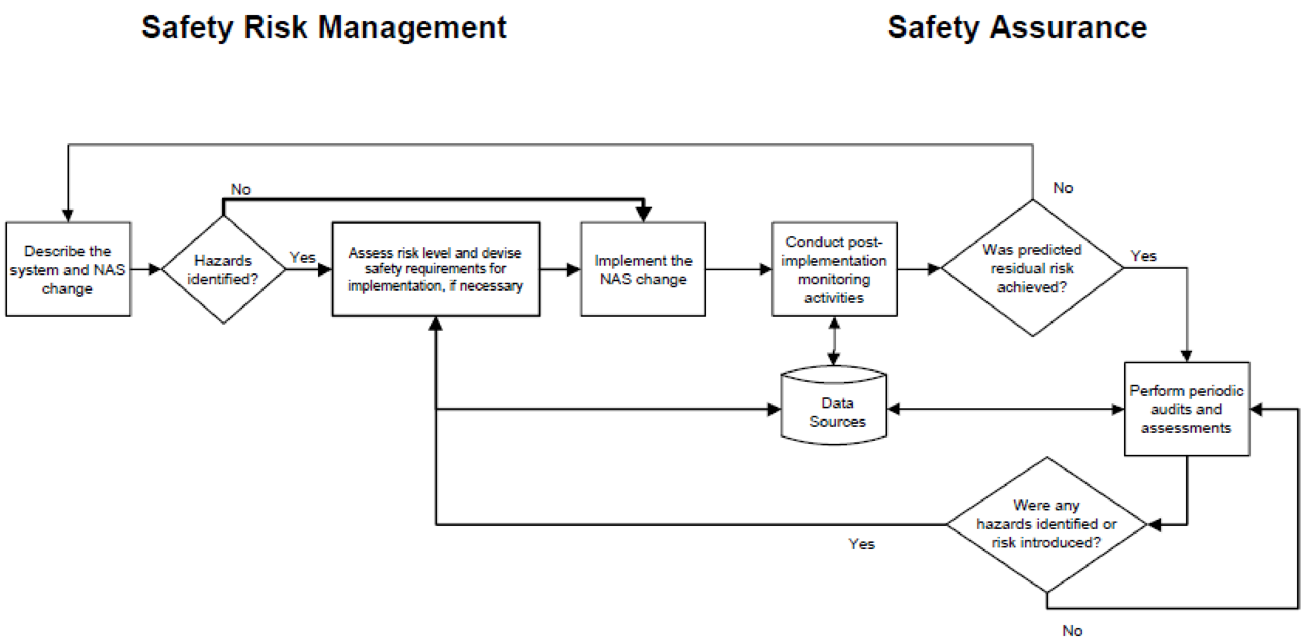


Figure 6.1: Closed-Loop Process for Managing Safety Risk

6.2.2 AJI's Role in Safety Data Collection and Evaluation

AJI obtains safety data through various sources within and outside the FAA. AJI measures safety by tracking safety metrics to produce reports on NAS safety, which are shared with appropriate LOBs and/or external stakeholders.

6.2.3 Safety Data Collection and Reporting Processes

The FAA collects and reports on safety data from various sources in the NAS. Section 7 lists many of the existing FAA and ATO orders, processes, and databases related to safety data collection and reporting.

- FAA Order JO 7210.632, *Air Traffic Organization Occurrence Reporting*, provides specific direction regarding the recording, reporting, and investigation of air traffic incidents.
- FAA Order JO 6040.15, *National Airspace Performance Reporting System*, and FAA Order 6000.30, *National Airspace System Maintenance Policy*, cover reporting on the serviceability of ATO facilities and systems, such as failures and degradations of communications, surveillance, and other systems and equipment that affect safety. Maintenance guidelines, directives, checklists, configuration management, and the NAS Technical Evaluation Program all contribute to the periodic review and maintenance of equipment and procedures.
- The Safety Recommendation Reporting System provides FAA aviation safety inspectors with a method to develop and submit safety recommendations directly to the Office of Accident Investigation and Prevention. (See FAA Order 8020.16, *Air Traffic Organization Aircraft Accident and Aircraft Incident Notification, Investigation, and Reporting*.)

- The Risk Analysis Process[1] quantifies the level of risk present in any air traffic incident. It provides a method for consistent and coherent identification of risk elements and allows users to prioritize actions designed to reduce the effect of those elements. The process uses the Risk Analysis Tool developed by EUROCONTROL to analyze each Risk Analysis Event (RAE). RAEs are assessed by a panel of air traffic and flight operations personnel (e.g., controllers and pilots rated for air transport). This panel is responsible for conducting the analysis of RAEs and coordinating the post-assessment reporting, mitigating, and tracking. The Risk Analysis Tool produces a numerical value of severity and repeatability on a risk matrix. The Risk Analysis Tool also captures any associated causal, systemic, and contributing factors.
- The Aviation Risk Identification and Assessment (ARIA) automated system identifies and assesses latent risk in the NAS and helps prioritize event analysis. A Barrier Analysis Review (BAR) is the assessment of safety data to determine systemic risk and includes an evaluation of safety barrier resiliency. The aggregate data produced by this process assists in the identification of systemic trends and potential risk in the NAS. Referred ARIA Reports, potential operational risk identified during the Quality Assurance (QA) validation process, service area QA manager referral, National Air Traffic Controllers Association service area or national safety representative referral, AJI Headquarters manager referral, and random QA selections are all means by which safety data may be referred for BAR.

Several non-punitive, voluntary reporting programs allow pilots and ATO personnel to report an incident or event without reprisal. These programs include the Aviation Safety Action Program (refer to the Air Traffic Safety Oversight Service Safety Oversight Circular 07-04, *Aviation Safety Action Program (ASAP) for Credentialed ATO Personnel*), the Aviation Safety Reporting Program, the Technical Operations Safety Action Program, and the Air Traffic Safety Action Program. They are designed to foster consistent reporting and higher quality data.

Other mechanisms employed by the FAA for employees to report issues include the Unsatisfactory Condition Report program, the Aviation Safety Hotline, and the Administrator's Hotline. Both hotlines can be reached by calling 1-800-255-1111.

1. FAA Order JO 7210.633 removed Risk Analysis Events (RAEs) and the process for notification and interviews associated with RAEs. Any reference to RAEs in this SMS Manual are for research and historical purposes only.

7.1 Safety Data and Information Repositories

Federal Aviation Administration (FAA) employees populate several aviation safety databases with information regarding National Airspace System (NAS) safety events and serviceability. Many professionals use aviation safety data and information as input for the development of NAS safety enhancements. For assistance in collecting safety data, contact the Safety (AJI) Safety Analysis Group, AJI-32. Sources for gathering safety data and information include:

- National Transportation Safety Board (NTSB) recommendations;
- FAA recommendations;
- Air Traffic Safety Oversight Service compliance issues;
- Requirements for new communication, navigation, surveillance, and automation services to enhance or expand airspace management;
- Unsatisfactory Condition Reports;
- Employee suggestions;
- Applications for procedural changes;
- Research and development;
- Acquisition of new systems and equipment;
- Industry advocacy;
- Participation in international forums;

Table 7.1 provides an overview of various safety databases and recording systems used by the FAA, and Table 7.2 outlines data types and applicable reporting requirements.

Table 7.1: Safety Databases and Reporting Systems

System Name	Overview
Mandatory Reporting Data	
Accident/Incident Data System	The Accident/Incident Data System contains data records for all general aviation and commercial air carrier incidents since 1978.
Air Traffic Quality Assurance database	Formerly known as the National Airspace Incidents Monitoring System, the Air Traffic Quality Assurance database is a collection of databases specific to the following subjects: Near Mid-Air Collisions (NMACs), pilot deviations, vehicle/pedestrian deviations, and Area Navigation / Required Navigation Performance deviations. The NMAC database contains reports of in-flight incidents where two aircraft have closed to an unsafe distance but avoided an actual collision. The pilot deviation database contains incident reports in which the actions of a pilot violated a Federal Aviation Regulation or a North American Aerospace Defense Command Air Defense Identification Zone tolerance. The vehicle/pedestrian deviation database contains incident reports of pedestrians, vehicles, or other objects interfering with aircraft operations on runways or taxiways.
Aviation Risk Identification and Assessment (ARIA) System	ARIA is an automated system that helps employ risk-based, data-driven decision-making, facilitating better insight into potential risk in the NAS via the Barrier Analysis Review process, which assesses severity, likelihood, and barrier effectiveness in Referred ARIA Reports. Barrier analysis is also used to identify and assess factors (mitigating, aggravating, or observed) for air traffic operations where at least one aircraft is receiving Air Traffic Control (ATC) services.
Aviation Safety Information Analysis and Sharing (ASIAS) System	ASIAS is a data warehouse and integrated database system. It enables users to perform queries across multiple databases and display queries in useful formats. It includes accidents, incidents, and pilot reports of NMACs.
Compliance Verification Tool (CVT)	The CVT replaces the Facility Safety Assessment System. Facilities conduct internal compliance verifications and enter the information in the tool. The Quality Control groups in the Service Units conduct external compliance verifications and enter the information in the tool. Service delivery points also develop risk mitigation plans that communicate how specific risks will be mitigated for all checklist items contained in the CVT determined to be noncompliant.
Comprehensive Electronic Data Analysis and Reporting (CEDAR)	The CEDAR system provides an electronic means of assessing employee performance, managing resources, and capturing safety-related information and metrics. The tool provides a standard interface for the collection, retrieval, and reporting of data from multiple sources. It also automates the creation, management, and storage of facility activities, events, briefing items, Quality Assurance Reviews, Technical Training discussions, and FAA forms.
Facility Safety Assessment System	The Facility Safety Assessment System is a national database that contains historical information related to the Facility Safety Assessment process. This information includes evaluation checklists, reports, facility information, tracking information, and response data.
Integrated NAS Technical Evaluation Program Application	This national database contains reports, findings, and mitigation plans from NAS Technical Evaluation Program audits and assessments. It is maintained by the NAS Quality Assurance and Performance Group in the Services Management Group.
NTSB Accident and Incident Database	The NTSB accident and incident database is the official repository of aviation accident data and causal factors. In this database, personnel categorize events as accidents or incidents.

System Name	Overview
Safety Management Tracking System	SMTS is the official repository for all ATO SRM documentation.
Mandatory Reporting Data	
Facility Directives Repository	This database contains Letters of Agreement, Standard Operating Procedures, and facility orders for all facilities nationwide.
Operations Network	The Operations Network is the official source of NAS air traffic operations and delay data. The data collected through the Operations Network are used to analyze the performance of the FAA's ATC facilities' traffic count and delay information, airport traffic control tower and Terminal Radar Approach Control operations, etc.
Performance Data Analysis and Reporting System (PDARS)	PDARS calculates a range of performance measures, including traffic counts, travel times, travel distances, traffic flows, and in-trail separations. It turns these measurement data into information useful to FAA facilities through an architecture that features: • Automatic collection and analysis of radar tracks and flight plans, • Automatic generation and distribution of daily morning reports, • Sharing of data and reports among facilities, and • Support for exploratory and causal analysis.
Risk Analysis Tool	FAA Order JO 7210.633, *Air Traffic Organization (ATO) Quality Assurance (QA)*, removed Risk Analysis Events (RAEs) and the process for notification and interviews associated with RAEs. Any references to RAEs in this Safety Management System Manual are for research and historical purposes only. RAE severity indicators are as follows: a. **Proximity.** Failure transition point of 50 percent of required separation or less. b. **Rate of Closure.** Failure transition point greater than 205 knots or 2,000 feet per minute (consider both aspects and utilize the higher of the two if only one lies above the transition point). c. **ATC Mitigation.** ATC able to implement separation actions in a timely manner. d. **Pilot Mitigation.** Pilot executed ATC mitigation in a timely manner.
Voluntary Reporting	
Air Traffic Safety Action Program (ATSAP)	ATSAP is a non-punitive, voluntary reporting program modeled after the Aviation Safety Action Program for employees delivering air traffic services. It allows employees to submit safety concerns and deficiencies so issues can be resolved before a major error occurs. This voluntary reporting helps promote a strong safety culture within the Air Traffic Organization (ATO).
Aviation Safety Action Program (ASAP)	ASAP promotes voluntary reporting of safety issues and events that come to the attention of employees of certain certificate holders. It includes enforcement-related incentives to encourage employees to voluntarily report safety issues, even though the issues may involve an alleged violation of Title 14 of the Code of Federal Regulations.
Aviation Safety Reporting System (ASRS)	ASRS collects voluntarily submitted aviation safety incident/situation reports from pilots, controllers, and other personnel. It identifies system deficiencies and issues messages to alert individuals in a position to correct the identified issues.
TechNet	The TechNet website provides a means for expediently distributing NAS operational information within the FAA. It contains information such as NAS delay information by service (e.g., automation, surveillance, navigation, and communication) and active equipment outages (i.e., full interruptions to service).

System Name	Overview
Technical Operations Safety Action Program (T-SAP)	T-SAP is a voluntary, non-punitive safety reporting program for ATO Technical Operations personnel. Employees at the point of service have a unique understanding of safety and can better identify threats and risks to their particular operations. By studying the data gained from voluntary reports, safety issues can be more efficiently identified and mitigated.

Table 7.2: Data Types and Applicable Reporting Requirements

Data	Overview	References
Aircraft incident or accident	This order contains reporting requirements regarding safety issues, concerns, incidents, and accidents.	FAA Order JO 8020.16, *Air Traffic Organization Aircraft Accident and Accident Incident Notification, Investigation, and Reporting*
Mandatory occurrence reports	This order mandates that personnel collect and analyze data concerning air traffic incidents.	FAA Order JO 7210.632, *Air Traffic Organization Occurrence Reporting*
Oceanic altitude and navigation errors	This order establishes procedures for processing reports and for collecting system data for analysis.	FAA Order JO 7210.632, *Air Traffic Organization Occurrence Reporting*
Safety recommendations	This order establishes procedures for Aviation Safety Inspectors to report safety recommendations directly to the Office of Accident Investigation and Prevention.	FAA Order JO 8020.16, *Air Traffic Organization Aircraft Accident and Aircraft Incident Notification, Investigation, and Reporting*
Significant system events	This order mandates that significant events be reported and contributes to daily system performance and incident reporting.	FAA Order JO 6030.41, *Technical Operations Notification of System and Service Interruptions and Other Significant Events*
System outages	This order mandates that outage reports be filed and contributes to daily system performance and incident reporting.	FAA Order JO 6040.15, *National Airspace Performance Reporting System (NAPRS)*
Unsatisfactory conditions	This order provides FAA employees with a means of informing management of unsatisfactory conditions.	FAA Order 1800.6, *Unsatisfactory Condition Report*
Voluntary Safety Reports	This order defines the policy and procedures for ATO Voluntary Safety Reports. It identifies the responsibilities of individuals and organizations and the requirements, expectations, and policies under which the identified programs operate.	FAA Order JO 7200.20, *Voluntary Safety Reporting Programs*
SMS Activities	This order mandates the ATO to report and share ATO SMS activities and results with the Air Traffic Safety Oversight Service.	FAA Order 1100.161, *Air Traffic Safety Oversight*

8.1 Definitions

Acceptable Level of Safety Risk. Medium or low safety risk.

Accident. An unplanned event or series of events that results in death; injury; or damage to, or loss of, equipment or property.

Active Failure. An error of omission or commission that is made in the course of a particular operation. An active failure can also be a known problem or a known mechanical deficiency or fault.

Acquisition Management System (AMS). A Federal Aviation Administration (FAA) policy dealing with any aspect of lifecycle acquisition management and related disciplines. The AMS also serves as the FAA's Capital Planning and Investment Control process.

Air Traffic Safety Oversight Service (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.

Analysis. The process of identifying a question or issue to be addressed, examining the issue, investigating then interpreting the results, and possibly making a recommendation. Analysis typically involves using scientific or mathematical methods for evaluation.

AOV Approval. The formal act of approving a National Airspace System (NAS) change submitted by a requesting organization. This action is required prior to the proposed NAS change being implemented.

Assessment. A process of measuring or judging the value or level of something.

Assumptions. Conclusions based on the presumed condition of a system or system state—not documented facts, desired outcomes, or mitigations.

Audit. A review of an organization's safety programs or initiatives to verify completion of tasks and to determine the organization's compliance with FAA directives and procedures.

Aviation Risk Identification and Assessment (ARIA). An automated system that helps employ risk-based, data-driven decision-making, which facilitates better insight into potential risk in the NAS.

Barrier Analysis Review (BAR). The process used to assess severity, likelihood, and barrier effectiveness in Referred ARIA Reports. Barrier analysis is also used to identify and assess factors (mitigating, aggravating, or observed) for air traffic operations where at least one aircraft is receiving Air Traffic Control (ATC) services.

Baseline. A set of conditions and systems that were operational as of March 14, 2005, and serves as the reference point for safety oversight within the Air Traffic Organization (ATO). It encompasses the following components: 1) Safety Standards: Includes all safety standards documented in written directives, orders, and procedures; 2) Controlled Airspace and Surface Areas: Encompasses all airspace and surface areas managed by the ATO; 3) Navigational and

Air Traffic Control Systems: Consists of the existing navigational systems and air traffic control services; and 4) Personnel Training and Certification System: Constitutes the current system for training and certifying ATO personnel. All modifications to systems included in the baseline must adhere to the procedures outlined in the ATO Safety Management System (SMS). It is important to note that the safety level established by the baseline is not inherently considered an acceptable level of safety; continuous evaluation and improvement are necessary. Inclusion of a system/service in the baseline does not exempt it from Safety Risk Management (SRM). Typically, it will require SRM.

Bounding. A process of limiting the analysis and assessment of a change or system to only the elements that affect or interact with each other to accomplish the central function of that change or system.

Cause. The origin of a hazard.

Change Proponent. An individual, Program Office, facility, or organization within the FAA that has identified the need for SRM or has proposed or is sponsoring a NAS change or means to address an identified existing safety issue. The SRM panel members are selected at the discretion of the change proponent and/or SRM panel facilitator.[1]

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

Compliance Audit. An audit that evaluates conformance to established criteria, processes, and work practices. The objective of a compliance audit is to determine whether employees and processes have followed established policies and procedures.

Continuous Loop. SRM processes are repeated until the safety risk associated with each hazard is acceptable and has met its predicted residual risk.

Concurrence. The concurrence signature is used to represent a technical review of the SRM document and to confirm the rationale used throughout is consistent with the SRM process. The concurrence signature comes from an SRM expert who is well versed in this Safety Management System (SMS) Manual and familiar with the terminology and processes therein.

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

Confirmation. The act of using a written response from a non–SRM panel attendee to confirm the integrity of a specific item or assertion.

Consensus. The judgement arrived at by a majority of panel members.

Control. Any means currently reducing a hazard's causes or effects. (See "Mitigation.")

Credible. It is reasonable to expect that the assumed combination of conditions that define the system state will occur within the operational lifetime of a typical ATC system (i.e., 30 years).

1. Employees of FAA Contract Towers can serve as change proponents on an SRM panel.

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.

Current Risk. The composite of severity and frequency of a hazard's effects in the present state.

Development Assurance. All the planned and systematic actions used to substantiate, at an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable approval or certification basis.

DIAAT Process. A process containing five steps for conducting Safety Risk Management. This process contains the following steps: Describe the System, Identify Hazards, Analyze Risk, Assess Risk, and Treat Risk.

Dissention. If any SRM panel member disagrees with the SRM panel's official findings (i.e., group consensus cannot be reached), that panel member should provide the nature and summary of the disagreement for inclusion in this part of the SRM document.

Effect. The real or credible harmful outcome that has occurred or can be expected to occur if the hazard occurs in the defined system state.

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

Error-Tolerant System. A system that is 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. An error-tolerant design is the human equivalent of a fault-tolerant design.

Existing Safety Issue. Existing contributing factors or findings that led to, or could lead to, an unsafe outcome.

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.

Fail Operational. A system designed such that if it sustains a fault, it still provides a subset of its specified behavior.

Fail Safe. A system designed such that if it fails, it fails in a way that will cause no harm to other devices or will not present a danger to personnel.

Fault Tolerance. The ability of a system to respond without interruption or loss of capabilities in the event of an unexpected hardware or software failure.

Frequency. An expression of how often a given effect occurs.

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 prerequisite to an accident or incident.

Hazard Analysis Worksheet (HAW). A tool used to provide an initial overview of the hazard's presence in the overall flow of the operation.

Hazard Identification. The determination of the hazard scenarios and associated consequences (undesired events) as a result of introducing a new system into the NAS. This provides an intermediate product that expresses the hazards that will be used during risk analysis and assessment.

High Rigor of SRM. A level of SRM rigor/effort (i.e., depth and detail) that involves convening an SRM panel to complete the DIAAT process.

High-Risk Hazard. A hazard with an unacceptable level of safety risk; the NAS change cannot be implemented unless the hazard's associated risk is mitigated and reduced to medium or low.

Hull Loss. An aircraft that is destroyed / substantially damaged beyond economic repair, missing, or completely inaccessible.

Human-Centered. The structured process during concept and requirement 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; 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, environments, training, staffing, and personnel management for safe, comfortable, and effective human performance. (See FAA Order 9550.8, *Human Factors Policy*.)

Incident. An occurrence other than an accident that affects or could affect the safety of operations.

Initial Risk. The composite of the severity and likelihood of a hazard's effect, considering only controls and documented assumptions for a given system state. It describes the risk before any of the proposed mitigations are implemented.

Inquiry. The technique of asking questions and recording responses.

Inspection. The act of critically examining documents to determine the content and quality of a transaction, such as inspecting leases, contracts, meeting minutes, requirements, and organization policy.

Latent Failure. An error or failure with adverse consequences that may lie dormant within a system for a long time, becoming evident when combined with other factors.

Likelihood. The estimated probability or frequency, in quantitative or qualitative terms, of a hazard's effect or outcome.

Maintenance. Any repair, adaptation, upgrade, or modification of NAS equipment or facilities. This includes preventive maintenance.

Management Strategy. Actions designed to reduce or manage the risk associated with a NAS change or operation.

Mitigation. Any means to reduce the risk of a hazard.

National Airspace System (NAS). A complex system that is composed of airspace, airports, aircraft, pilots, air navigation facilities, and ATC facilities; communication, navigation, and surveillance services and supporting technologies and systems; operating rules, regulations, policies, and procedures; and people who implement, sustain, or operate the system components.

NAS Change. A modification to any element of the NAS that pertains to, or could affect, the provision of air traffic management and/or communication, navigation, and surveillance services.

Objective Evidence. Documented proof; the evidence must not be circumstantial and must be obtained through observation, measurement, testing, or other means.

Observation. The process of witnessing an organization’s process. It differs from a physical examination in that the auditor only observes the process; no physical evidence is obtained.

Operational Assessments. An assessment to address the effectiveness and efficiency of an organization. The objective of an operational assessment is to determine the organization’s ability to achieve its goals and accomplish its mission.

Opposing Opinion. An opinion submitted in writing if a Subject Matter Expert (SME) participating in an SRM panel disagrees with that SRM panel’s official findings; opposing opinions are attached to the SRM document as part of the distribution.

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

Physical Examination. The act of gathering physical evidence. It is a substantive test involving the counting, inspecting, gathering, and inventorying of physical and tangible assets, such as cash, plants, and equipment.

Preconditions. The system states or variables that must exist for a hazard or an accident to occur in an error-tolerant system.

Predicted Residual Risk. The risk that is estimated to exist after the safety requirements are implemented or after all avenues of risk mitigation have been explored.

Preliminary Hazard List (PHL). A hazard identification tool used to list all potential hazards in the overall operation. Development of a PHL typically begins with a brainstorming session among the individuals participating in the SRM panel.

Process. A set of interrelated or interacting activities that transform inputs into outputs.

Program Assessment. A Safety Assessment's review of an organization's safety programs or initiatives. Programs and initiatives include, but are not limited to, Service Area Quality Assurance (QA), Air Traffic Facility Quality Control, Runway Incursion Prevention Plans, Equipment Availability Programs, and Contractor QA programs for Federal Contract Towers (FCT).

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

Quality Assurance (QA). A program for the systematic monitoring and evaluation of the various aspects of a project, service, or facility to ensure that standards of quality are being met. It is a process to assess and review the processes and systems that are used to provide outputs (whether services or products) and to identify risks and trends that can be used to improve these systems and processes.

Quality Control. A process that assesses the output (whether a product or service) of a particular process or function and identifies any deficiencies or problems that need to be addressed.

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

Recording. The process of documenting the identified hazards and the associated safety information.

Redundancy. A design attribute in a system that ensures 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. A requirement 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.

Residual Risk. The level of risk that has been verified by completing a thorough monitoring plan with an achieved measurable safety performance target(s). Residual risk is the composite of the severity of a hazard's effect and the frequency of the effect's occurrence.

Risk. The composite of predicted severity and likelihood of the potential effect of a hazard.

Risk Acceptance. The confirmation by the appropriate management official that they understand the safety risk associated with the NAS change or existing safety issue and that they accept that safety risk into the NAS. Risk acceptance requires that signatures have been obtained for the safety requirements identified in the SRM document and that a comprehensive monitoring plan has been developed and will be followed to verify the predicted residual risk.

Risk Assumption Strategy. A risk management strategy used to accept the risk.

Risk Avoidance Strategy. A risk management strategy used to avert the potential occurrence and/or consequence of a hazard by either selecting a different approach or not implementing a specific proposal.

Risk Control Strategy. A risk management strategy used to develop options and take actions to lower the risk.

Risk Mitigation. Refer to “Mitigation.”

Risk Transfer Strategy. A risk management strategy used to shift the ownership of a risk to another party.

Safety. The state in which the risk of harm to persons or property damage is acceptable.

Safety Assurance. A set of processes within the SMS that verify that an organization meets or exceeds its safety performance objectives. These processes function systematically to determine the effectiveness of safety risk controls through the collection and analysis of data and assessment of information. Safety Assurance is one of the four components of the SMS.

Safety Culture. An organization’s shared action, values, and behaviors—modeled by its leaders and internalized and acted upon by its members—that demonstrate a commitment to safety over competing goals and demands.

Safety Case Lead (SCL). An expert in SMS policy and guidance that pertains to the ATO.

Safety Directive. A mandate from AOV to the 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 policies, processes, procedures, and programs used to manage safety risk in the provision of air traffic management and communication, navigation, and surveillance services.

Safety Margin. The buffer between the actual minimum-level requirement and the limit of the hardware or software system.

Safety Performance Indicators. Metrics identified to determine how risk mitigations are performing.

Safety Performance Monitoring. The act of observing the safety performance of the NAS to ensure an acceptable level of safety risk.

Safety Performance Targets. Measurable goals used to verify the predicted residual risk of a hazard. They should quantifiably define the predicted residual risk.

Safety Policy. The documented organizational policy that defines management’s commitment, responsibility, and accountability for safety. One of the four components of the SMS, Safety Policy identifies and assigns responsibilities and accountabilities to key safety personnel.

Safety Promotion. The communication and distribution of information to improve the safety culture and the development and implementation of programs and/or processes that support the integration and continuous improvement of the SMS within the ATO. One of the four components of the SMS, Safety Promotion allows the ATO to share and provide evidence of successes, best practices, and lessons learned.

Safety Requirement. A planned or proposed means to reduce a hazard’s causes or effects.

Safety Requirement Approval. Certification that the safety requirements can and will be implemented.

Safety Risk Management (SRM). A process within the SMS composed of the following steps: describing the system; identifying the hazards; and analyzing, assessing, and treating risk. One of the four components of the SMS, SRM includes requirements for defining monitoring strategies for the identified safety risk of the NAS. SRM complements Safety Assurance.

Severity. The credible consequence or impact of hazard's effect or outcome in terms of degree of loss or harm.

SRM Document. A document that records the SRM panel attendees' determinations for NAS changes and existing safety issues. It presents evidence supporting whether the NAS change and/or risk management strategies should be accepted by ATO or FAA management officials from a safety risk perspective.

SRM Document Approval (for SRM Documents With Hazards). Indication that the SRM document was developed in accordance with policy and guidance; hazards were systematically identified using a structured approach; risk was appropriately analyzed and assessed; if identified, safety requirements were deemed valid; safety performance targets or other methods to verify predicted residual risk were approved by the responsible Service Unit; and a monitoring plan was prepared. SRM document approval does not constitute acceptance of the risk associated with the NAS change or existing safety issue or approval to implement the NAS change.

SRM Document Approval (for SRM Documents Without Hazards). Indication that the SRM document was developed in accordance with policy and guidance, the NAS change did not introduce new hazards or increase safety risk, and the SRM document includes a detailed rationale to support the finding of no hazards.

SRM Panel. A meeting of a diverse group of SRM panel members, SMEs, observers, and facilitators from the various organizations affected by the NAS change or existing safety issue. They objectively identify potential hazards and effects associated with the NAS change or existing safety issue and provide findings and recommendations to decision-makers, which are captured in an SRM document.

SRM Panel Co-Facilitator. A person who shares responsibilities with the SRM panel facilitator in supporting the SRM panel.

SRM Panel Facilitator. A trained expert on the SRM process who moderates the deliberations of the SRM panel attendees from a neutral position. They invoke participation, mediate discussion, ensure any dissenting opinions are documented, keep the meeting organized and on topic, remain neutral throughout the process without advocating for a specific outcome, and may support the development of the SRM document.

SRM Panel Member. An SRM panel member is an FAA employee[2] or other representative (as specified in an FAA Memorandum of Agreement)[3] who objectively performs the SRM process. The SRM panel members are selected at the discretion of the change proponent and/or SRM panel facilitator.

SRM Panel Observer. An individual who is not part of the SRM panel meeting and does not participate in the deliberation process (only observes the proceedings). They have an objective to obtain a better understanding of the SRM process—not the NAS change or existing safety issue being addressed. SRM panel observers are permitted at the discretion of the change proponent.

Safety Risk 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. Safety risk tracking is the process of defining safety requirements, verifying implementation, and readdressing the risk to make sure the hazard meets its risk level requirement before being accepted.

Severity. The consequence or impact of a hazard's effect or outcome in terms of degree of loss or harm.

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.

SMS Continuous Improvement Plan. The plan that specifies the activities required for individual ATO Service Units to allocate sufficient resources toward the integration and maturation of the ATO SMS.

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

Stakeholder. A group or individual that is affected by or is in some way accountable for the outcome of a safety 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.

Subject Matter Expert (SME). An FAA employee or third-party stakeholder who serves as a technical expert on the NAS change, procedure, hardware/software, or proposed solution undergoing SRM. SMEs supplement the expertise of the SRM panel members to assist in the risk analysis, but they are not SRM panel members and do not make consensus-driven decisions when working through the SRM process.

System. Integrated elements that are combined in an operational or support environment to accomplish a defined objective. These elements include people, hardware, software, firmware, information, procedures, facilities, services, and other support facets.

2. Inclusive of FCT employees or other contractors who have been given explicit authority to represent (i.e., make decisions for / speak on behalf of) the FAA.

3. This includes FAA bargaining unit representatives or Department of Defense (DoD) representatives. Note: DoD representatives participate as panel members when DoD ATC procedures/airspace are impacted.

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

Tracking. The continued process of documenting the results of monitoring activities and the change's effect on the safety of the NAS.

Two-Phase Local SRM. A type of local SRM conducted only on NAS changes that meet the criteria in Section 3.3.3 of the ATO SMS Manual and that stakeholders suspect will have no potential to introduce hazards or increase safety risk, This approach involves conducting the "Describe the System" and "Identify Hazards" phase of the DIAAT process with a group of stakeholders and does not require the change proponent to convene an SRM panel unless the process uncovers the potential to affect safety risk in the NAS.

Unacceptable Level of Safety Risk. A high-risk hazard or a combination of medium/low risks that collectively increase risk to a high level.

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

8.2 Acronyms

ADS-B	Automatic Dependent Surveillance–Broadcast
AIS	Aeronautical Information Services
AJI	Safety
AJM	Program Management Organization
AJV	Mission Support Services
AJV-H	Enterprise Services Directorate
AJW	Technical Operations
AMASS	Airport Movement Area Safety System
AMS	Acquisition Management System
AOV	Air Traffic Safety Oversight Service
ARIA	Aviation Risk Identification and Assessment
ARP	Office of Airports
ARSR	Air Route Surveillance Radar
ARTCC	Air Route Traffic Control Center
ARTS	Automated Radar Terminal System
ASAP	Aviation Safety Action Program
ASDE	Airport Surface Detection Equipment
ASIAS	Aviation Safety Information Analysis and Sharing
ASR	Airport Surveillance Radar
ASRS	Aviation Safety Reporting System
ATC	Air Traffic Control
ATCRBS	Air Traffic Control Radar Beacon System
ATCT	Airport Traffic Control Tower
ATM	Air Traffic Management
ATO	Air Traffic Organization
ATO-SG	Air Traffic Organization Safety Guidance
ATSAP	Air Traffic Safety Action Program
BAR	Barrier Analysis Review

CAP	Corrective Action Plan
CAT	Category
CEDAR	Comprehensive Electronic Data Analysis and Reporting
CISP	Confidential Information Share Program
CNS	Communications, Navigation, and Surveillance
COMM	Communications
COO	Chief Operating Officer
CSA	Comparative Safety Assessment
CVT	Compliance Verification Tool
DoD	Department of Defense
eTPR	Electronic Technical Performance Record
FAA	Federal Aviation Administration
FCT	FAA Contract Tower
HAW	Hazard Analysis Worksheet
HMI	Hazardously Misleading Information
ICAO	International Civil Aviation Organization
IFR	Instrument Flight Rules
IMC	Instrument Meteorological Conditions
IOA	Independent Operational Assessment
LOA	Letter of Agreement
LOB	Line of Business
LOP	Letter of Procedure
MODES	Mode Select Beacon System
NAS	National Airspace System
NATCA	National Air Traffic Controllers Association
NAV	Navigation
NOTAM	Notice to Airmen
NCP	NAS Change Proposal
NMAC	Near Mid-Air Collision
NTSB	National Transportation Safety Board
OCS	Obstacle Clearance Surface
OHA	Operational Hazard Assessment
OSA	Operational Safety Assessment
PDARS	Performance Data Analysis and Reporting System
PHL	Preliminary Hazard List
POC	Point of Contact
PRD	Program Requirements Document
QA	Quality Assurance
RAE	Risk Analysis Event

RAP	Risk Analysis Process
RI	Runway Incursion
SCL	Safety Case Lead
SME	Subject Matter Expert
SMS	Safety Management System
SMTS	Safety Management Tracking System
SOC	Safety Oversight Circular
SOP	Standard Operating Procedure
SRM	Safety Risk Management
SRMGSA	Safety Risk Management Guidance for System Acquisitions
STARS	Standard Terminal Automation Replacement System
T-SAP	Technical Operations Safety Action Program
TCAS	Traffic Alert and Collision Avoidance System
TIS	Traffic Information Services
TRACON	Terminal Radar Approach Control
VFR	Visual Flight Rules
VMC	Visual Meteorological Conditions
WAM	Wide Area Multilateration

Annex A
Safety Risk Management Application and Guidance

Contents

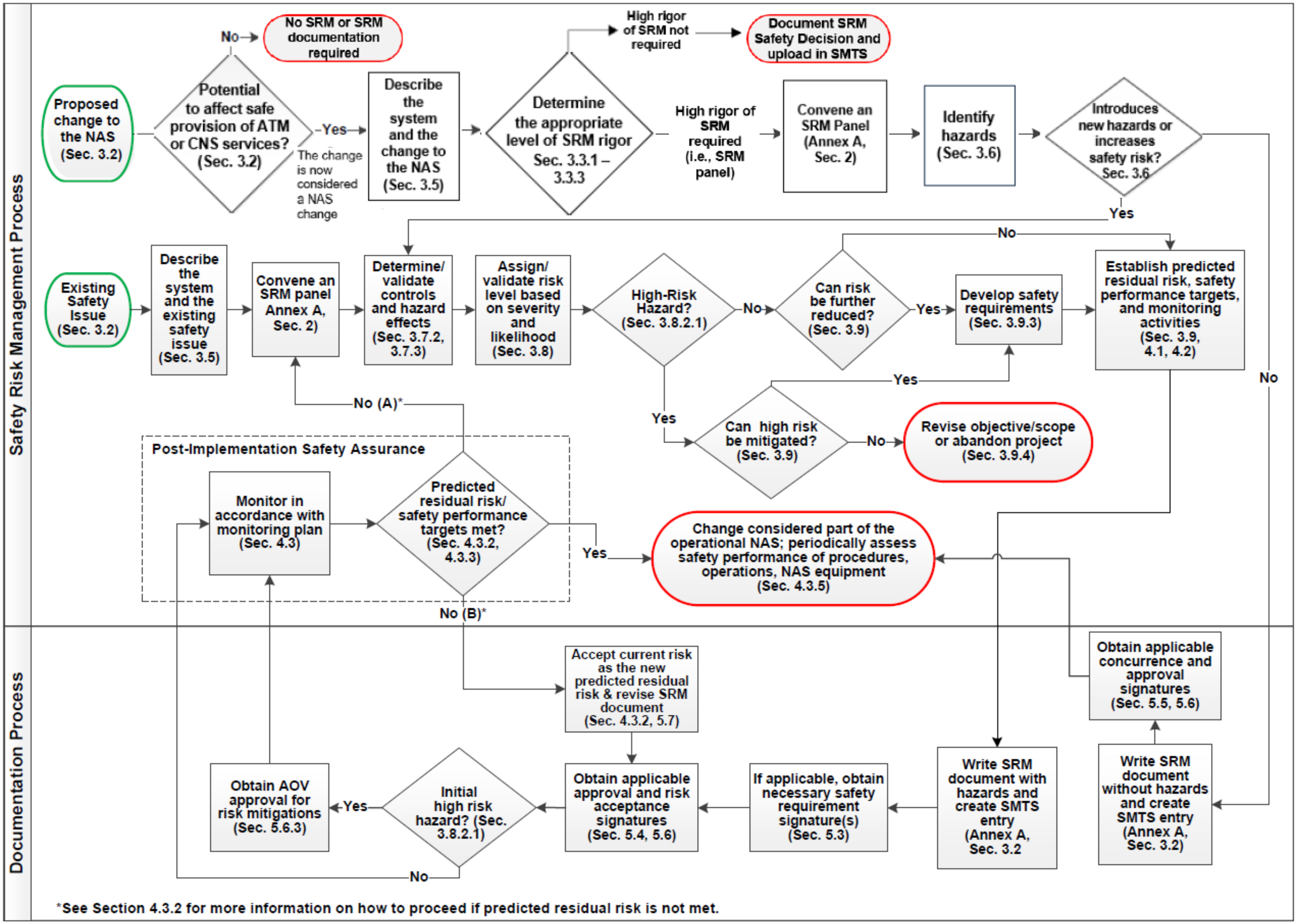


Figure A.1: Overview of the Safety Risk Management Process

1. Preparing for, Conducting/Convening, and Documenting a Safety Risk Management Effort

1.1 Overview

This section provides practical guidance for applying the Safety Risk Management (SRM) process, which is depicted in Figure A.1. This section outlines information regarding how to:

- Determining whether a proposed change is a National Airspace System (NAS) change
- Conducting the Preliminary Safety Assessment to determine whether high rigor of SRM (i.e., an SRM panel) is required,
- Preparing for and convening an SRM panel, and
- Producing the resulting SRM documentation.

1.2 Identifying NAS Changes and the Preliminary Safety Assessment

The scope of an SRM effort is based on the type and complexity of the proposed change or existing safety issue and its effect on the NAS. When an existing safety issue in the NAS is identified, the change proponent must convene an SRM panel to address the identified safety risk. (See Section 1.2.1 and Section 2 of this annex for guidance on SRM for existing safety issues.) When the trigger for SRM is a proposed change, however, the following steps are essential for identifying SRM requirements associated with the change. performing the Preliminary Safety Assessment—through which the appropriate rigor of SRM (i.e., the appropriate depth and detail) is determined for the proposed change / existing safety issue. (This information is also important for planning and preparing for subsequent SRM activities related to the proposed change or existing safety issue.):

1. Determine whether the proposed change is a NAS change. (See Air Traffic Organization (ATO) Safety Management System (SMS) Manual Sections 3.1 and 3.2 for additional guidance.) The change proponent must determine whether a proposed change pertains to or has the potential to affect the safe provision of Air Traffic Management (ATM) or Communication, Navigation, and Surveillance (CNS) (ATM/CNS).
   - If it **does not**, the proposed change **is not** a NAS change, and no further SRM or SRM documentation is required. (However, completion of the "Describe the System" phase of the DIAAT process may be helpful in making this determination, and though not required to do so, change proponents may choose to document the system and change information in an SRM Safety Decision. See Section 3.2 of this annex for more documentation information.)
   - If it **does**, the proposed change **is** a NAS change, and steps 2 through 5 must be completed, as applicable.
2. For NAS changes, conduct the Preliminary Safety Assessment:
   i. Complete the "Describe the System" phase of the DIAAT process by describing the NAS change, its scope, and the operational system in which the change will occur. (See ATO SMS Manual Section 3.5 for information on this DIAAT phase.)
   ii. Consider the NAS change's potential to introduce hazards or increase safety risk to determine the appropriate rigor of the SRM effort (e.g., whether an SRM panel will be required for the safety analysis):

   iii. Determine the appropriate rigor of the SRM effort (e.g., determine whether the NAS change will require safety analysis by an SRM panel). See Section 1.2.2 of this Annex for guidance on completing this step.)

3. If an SRM panel **is required**, identify an SRM panel facilitator and appropriate SRM panel attendees.
4. If an SRM panel **is not required**, document this determination in an SRM Safety Decision and upload it in Safety Management Tracking System (SMTS).

To support these activities, each of which are detailed below, the change proponent for the SRM effort should consult their Service Center Quality Control Group; the Safety (AJI) Safety Engineering Team, AJI-314, Manager (who can be contacted through the ATO SMS mailbox); or a local safety Point of Contact (POC) when initiating the process.

1.2.1 Describe the System and NAS Change or Existing Safety Issue

The change proponent must conduct the "Describe the System" phase of the DIAAT process to properly define the purpose and scope of the NAS change or existing safety issue using input from technical experts. The change proponent should consider the impact of the NAS change on relevant NAS equipment, operations, and procedures. This includes defining:

- The NAS change or existing safety issue,
- The system state(s) in which the change will be operational / in which the existing safety issue exists,
- Assumptions (not controls), and
- The components of the 5M Model.

See ATO SMS Manual Section 3.5 for more guidance on the "Describing the System" phase of the DIAAT process.

1.2.2 Determine the Appropriate Rigor of SRM for a NAS Change

After identifying that a proposed change is a NAS change and completing the "Describe the System" phase of the DIAAT process, the change proponent must continue the Preliminary Safety Assessment to determine the appropriate rigor of the SRM effort (i.e., the appropriate depth and detail of the safety analysis). This requires the change proponent to consider whether the NAS change has the potential to introduce hazards or increase safety risk by conducting a simple analysis of the system and change description. Such analysis may be difficult if the change or the system in which it will occur interfaces or interacts with other NAS systems, which is more likely as systems in the NAS continue to evolve. Change proponents are encouraged to use the information in ATO SMS Manual Section 3.5.2 to address potential gaps created by the NAS change within the current system and to contact their Service Center or an AJI Safety Case Lead (SCL) if they need additional guidance. Additionally, the change proponent may use the information in ATO SMS Manual Sections 3.3.1, 3.3.2, and—for qualifying local changes—3.3.3 to determine the appropriate rigor of the SRM effort and identify the required output SRM documentation. The change proponent should use all available resources when evaluating potential sources of risk. Evaluating such sources may involve consulting SRM or technical experts from relevant agency offices or coordinating with affected stakeholders (e.g., local personnel) to identify the potential safety impacts.

NAS changes that do not deviate from existing organizational standards, requirements, and protocols and for which the change proponent identifies no potential sources of hazards or increased safety risk commonly do not require any further SRM. However, the change proponent must document the findings from the completed “Describe the System” phase of the DIAAT (i.e., the description of the NAS change and the system in which it will occur) in an SRM Safety Decision with their reasoning for why the NAS change has no potential to introduce hazards or increase safety risk. (See Section 3.2 of this annex for documentation requirements.)

When a NAS change is local and meets the criteria defined in ATO SMS Manual Section 3.3.3.2, the change proponent may conduct Two-Phase Local SRM to determine whether the NAS change has the potential to introduce hazards or increase safety risk without the need to conduct further SRM (e.g., an SRM panel). (Guidance for conducting Two-Phase Local SRM is in ATO SMS Manual Section 3.3.3.3.) If this Two-Phase Local SRM identifies no potential for the NAS change to introduce hazards or increase safety risk, the change proponent must simply document these findings in an SRM Safety Decision and upload it in SMTS. However, if the Two-Phase Local SRM process identifies a potential for the NAS change to introduce hazards or increase safety risk, the change proponent must convene an SRM panel and upload all SRM documentation in SMTS.

In the case that high rigor of SRM is required or an SRM panel is convened, the panel determines the safety risk associated with the NAS change—not its suitability, validity, or necessity. Panel deliberations must not be used to define what the NAS change should be or to change the purpose or intent of the NAS change defined by the organization(s) sponsoring the NAS change. After the SRM panel concludes, the findings of the DIAAT process (including the “Describe the System” phase earlier completed) are recorded in an SRM Document With or Without Hazards. (See Section 3.3 of this annex for SRM documentation requirements.)

2. Preparing For and Convening an SRM Panel

2.1 Identifying SRM Panel Attendees

When an SRM panel will convene, the change proponent works closely with the SRM panel facilitator/co-facilitator to identify the SRM panel attendees necessary to perform SRM. The size and composition of the SRM panel will vary based on the type and complexity of the proposed NAS change or existing safety issue, and it should be limited to an appropriately sized yet diverse team of stakeholders and Subject Matter Experts (SMEs). A stakeholder is considered to be an entity that could be affected by the proposed NAS change or existing safety issue from a safety risk perspective (i.e., an entity responsible for any of the following tasks: implementing the NAS change when approved, accepting the residual risk, implementing safety requirements, or affirming controls).

The change proponent, with the SRM panel facilitator, should obtain information on the knowledge, experiences, and positions of each attendee. The following list, though not all-inclusive, provides types of experts to consider for participation on an SRM panel:

- Employees directly responsible for developing the NAS change or managing the existing safety issue,
- Employees with current knowledge of and experience with the system or NAS change,
- Hardware/Software engineering and/or automation experts (to provide knowledge on equipment performance),

- Human factors specialists,
- Systems specialists,
- System operators,
- Employees skilled in collecting and analyzing hazard and error data and using specialized tools and techniques (e.g., operations research, data, and human factors),
- Quality Control / Quality Assurance employees (to help ensure that the safety performance target is measurable and auditable or to help develop an alternate means to verify predicted residual risk),
- Air traffic procedures specialists,
- Information and cyber-security specialists,
- Third-party stakeholders (e.g., pilots, pilot organizations, and industry representatives),
- Air traffic controllers,
- Maintenance technicians,
- Traffic management specialists, and
- Bargaining unit representatives.

The 5M Model is required and is a useful tool for identifying potential SRM panel members and SMEs. Note that it may be necessary to elevate a request for participation to an appropriate management level to ensure participation by all affected stakeholders.

Any SRM panel meeting attendee should fulfill one of the roles specified in the following subsections.

2.1.1 Change Proponent

A **change proponent** is an individual, Program Office, facility, or organization within the Federal Aviation Administration (FAA) that has identified the need for SRM or has proposed or is sponsoring a NAS change or means to address an existing safety issue.

Among other responsibilities, the change proponent works with the SRM panel facilitator to define the purpose and scope of the NAS change or existing safety issue, capture the safety findings from the SRM panel meeting in an SRM document, and ensure that the SRM document is recorded in SMTS. The change proponent may record the information directly, designate a responsible individual, or work with the SRM panel facilitator or organization responsible for accepting safety risk to enter the SRM document into SMTS.

Unless circumstances warrant doing so, the change proponent should not function as an SRM panel member at their SRM panel.

2.1.2 SRM Panel Facilitator

An **SRM panel facilitator** is a trained expert on the SRM process who moderates the deliberations of the SRM panel attendees from a neutral position.

The change proponent selects or requests an SRM panel facilitator. After, the change proponent and the facilitator (and co-facilitator if one is identified) will have an initial meeting to prepare for the SRM panel. During this time, the facilitator will provide a briefing to the change proponent on the SRM process and work with the change proponent to develop the scope of the SRM panel. The SRM panel facilitator should also become well-versed in the subject matter (e.g., by requesting briefings and collecting all available and relevant safety information), as necessary, before the SRM panel convenes.

This coordination and preparation between the change proponent and facilitator/co-facilitator results in the development of a briefing package to provide to SRM panel attendees before the panel meeting. The briefing package should include all relevant information about the NAS change or existing safety issue, the SRM panel meeting invitation, an agenda, briefing materials, and directions to the meeting venue.

An effective SRM panel facilitator ensures the SRM process is followed in an unbiased manner and works to achieve consensus, a judgement by a majority of panel members. They invoke participation, mediate discussion, ensure differences of opinions are documented, keep the meeting organized and on topic, and remain neutral throughout the process without advocating for a specific outcome. The facilitator (or their designee) may assist the change proponent in writing the SRM document, which describes the safety findings of the SRM panel meeting. Facilitator duties and responsibilities must be discussed with the change proponent and communicated to the SRM panel attendees.

2.1.2.1 SRM Panel Co-Facilitator

An **SRM panel co-facilitator** is a person who shares responsibilities with the SRM panel facilitator in supporting the SRM panel.

An SRM panel co-facilitator, if one is assigned, assists the facilitator. A co-facilitator is especially helpful when the panel size exceeds 12 attendees and/or the subject matter is complex. Like the facilitator, the co-facilitator (or their designee) may assist the change proponent in writing the SRM document describing the safety findings of the SRM panel meeting. Co-facilitator duties and responsibilities must be discussed with the change proponent and communicated to the SRM panel attendees.

2.1.2.2 Facilitation by AJI Safety Case Leads

An AJI SCL is an expert in SMS policy and guidance that pertain to the ATO. They may facilitate SRM efforts for existing safety issues and NAS changes that meet any of the following criteria:

- It has a high (potentially political, economic, or financial) impact on the FAA, the NAS, or the flying public.
- It is the result of financial or operational decisions made by FAA executive management, cabinet-level executives, or Congress.
- The NAS change is a proposed means of addressing any safety issues identified as high-priority safety issue by AJI.
- The NAS change modifies safety policy that must be incorporated in a directive.
- It can or does present operational or technical conflicts to multiple affected Service Units or FAA Lines of Business (LOBs).

2.1.3 SRM Panel Member

An **SRM panel member** is an FAA employee[1] or other representative (as specified in an FAA Memorandum of Agreement)[2] who objectively performs the SRM process.

An SRM panel member represents the program, facility, organization, or constituency potentially affected by the safety risk, the safety requirements associated with the proposed NAS change and/or the existing safety issue. Among other responsibilities, SRM panel members evaluate safety risk associated with the NAS change or existing safety issue objectively, thoroughly, and fairly; do not debate the validity of the NAS change; and review and comment on SRM documents.

2.1.4 SME

An **SME** is an FAA employee or third-party stakeholder who serves as a technical expert on the NAS change, procedure, hardware/software, or proposed solution undergoing SRM. SMEs share data, detailed information, and experience about the subject being discussed during the SRM panel meeting; partake in technical dialogue with SRM panel members; and review and comment on the aspects of SRM documents for which their expertise is applicable. SMEs supplement the expertise of the SRM panel members to assist in the risk analysis, but they are not SRM panel members and do not make consensus-driven decisions when working through the SRM process (e.g., when determining severity, likelihood, initial risk, predicted residual risk, and developing the Monitoring Plan).

Note: In other areas of the ATO SMS Manual, the term “subject matter expert” is used generically. Each SRM panel attendee is expected to have technical knowledge in a subject area that would suggest their participation in the panel meeting is appropriate.

2.1.5 SRM Panel Observer

An **SRM panel observer** is an individual who is not part of the SRM panel meeting and does not participate in the deliberation process (only observes the proceedings).

An observer has an objective to obtain a better understanding of the SRM process—not the NAS change or existing safety issue being addressed. They are not active members of the SRM panel meeting; do not provide input during the deliberations; and, like all other attendees, may not use electronic recording devices during the panel meeting. The presence of panel observers is permitted at the discretion of the change proponent.

2.1.5.1 Air Traffic Safety Oversight Service Attendance

In accordance with FAA Order 1100.161, *Air Traffic Safety Oversight*, the ATO must notify the Air Traffic Safety Oversight Service (AOV) of all planned SRM panels via email to the ATO SMS mailbox.) AOV may, at its discretion, be an observer for an SRM panel. The SRM panel facilitator or change proponent must evaluate the NAS change or existing safety issue to determine whether it will require approval or acceptance from AOV. If AOV approval or acceptance is required, then the SRM panel facilitator must coordinate with AJI to ensure compliance with AOV requirements. Contact the Manager of the Safety Management Group, AJI-31, for guidance, if necessary.

1. Inclusive of federal contract tower employees or other contractors who have been given explicit authority to represent (i.e., make decisions for / speak on behalf of) the FAA.

2. This includes FAA bargaining unit representatives or Department of Defense (DoD) representatives. Note: DoD representatives participate as panel members when DoD Air Traffic Control procedures / airspace are impacted.

2.1.5.2 Guidance for Bargaining Unit Participation
When selecting SRM panel attendees, adhere to the Collective Bargaining Agreement between the FAA and affected bargaining unit representatives. When a NAS change or existing safety issue crosses Service Area boundaries and LOBs, the change proponent must ensure Enterprise Services Directorate, AJV-H, Technical Labor and Management Development personnel are notified via email to the ATO SMS mailbox.

Ensure that all facilities, including their respective bargaining units, are given notification of the upcoming SRM panel. Labor organizations, such as the National Air Traffic Controllers Association and Professional Aviation Safety Specialists, represent several different bargaining units (engineers, controllers, attorneys, etc.). In some cases, multiple bargaining units may need to attend the panel to ensure that the appropriate expertise is available. Multiple bargaining unit members may attend the SRM panel, but only one member may act as an SRM panel member and participate in the consensus-driven deliberations. Additional personnel from that bargaining unit must fulfill a different panel role (e.g., SME, observer).

For assistance finding a labor union representative, contact AJV-H Technical Labor and Management Development via email to the ATO SMS mailbox for more information.

2.1.5.3 Participation on SRM Panels Outside of a Service Unit or the ATO
ATO employees are often requested to participate as stakeholders or SMEs on SRM panels sponsored by organizations outside of their Service Unit or the ATO. It is important to support these requests, whether they originate within or outside of the ATO. Participation as an SME or stakeholder does not necessarily mean that the organization represented by an SRM panel member is responsible for developing or implementing safety requirements, accepting risk, or approving the SRM document.

When requesting the participation of an ATO Service Unit, the requestor should contact the appropriate Program Office or Service Unit for coordination.

2.2 Convening and Conducting the SRM Panel
Following the identification and invitation of SRM panel attendees, the SRM panel convenes. On the first day of the SRM panel meeting, the SRM panel facilitator or a designee must present an SRM panel orientation that includes:

- The agenda for the meeting,
- A summary of the goals and objectives for the SRM panel,
- A brief review of the SRM process,
- SRM panel ground rules,
- The method(s) by which the SRM panel will identify hazards (if known), and
- A draft or summary of the “Current System” and “Description of Change” sections of the SRM document, if available, provided by the change proponent (see Sections 3.2.3 and 3.2.4 of this annex).

2.2.1 SRM Panel Meeting Logistics
The SRM panel facilitator may perform or delegate the function of time-keeper in order to manage start times and breaks. The facilitator may also delegate the recording of meeting notes, the writing of the SRM document, and the provision of audio/visual support.

The SRM panel should be conducted using in-person meetings, if possible; however, stakeholders can participate in SRM panel meetings via other methods, such as web meetings or teleconferences. In the event that the invited stakeholders cannot provide representation on an SRM panel, consult with the change proponent and, if feasible, continue the SRM panel as scheduled. The findings should then be forwarded to the absent stakeholders to gather additional input, comments, or concerns. If it is not feasible to conduct or continue the SRM process without the representation of the stakeholder in question (i.e., if the perspective of the stakeholder in question is critical to the validity and defensibility of the safety risk analysis), the change proponent must reschedule the SRM panel.

2.2.2 SRM Panel Deliberations

During the SRM panel, the SRM panel facilitator will lead attendees in objectively examining, identifying, and mitigating potential safety hazards and effects associated with the NAS change or existing safety issue. If hazards are identified, the SRM panel facilitator will guide the attendees through the five-step DIAAT process using the Hazard Analysis Worksheet (HAW) and monitoring plan (see Sections 3.2.6 and 3.2.7 of this annex).

SRM panel members should strive for unanimous agreement on risk determinations; however, there may be instances in which not all SRM panel members agree with the panel's consensus. In those cases, record the difference of opinions from the SRM panel members in the SRM document. Dissenting SRM panel members should provide, in writing, their own rationale and data for why their risk determination differs from that of the other SRM panel members. The written dissention must be included in the SRM document.

The SRM panel facilitator must mediate and assist SRM panel members in working through differences of opinion. The facilitator should be able to recognize, acknowledge, and use differences of opinion to help the SRM panel members consider different points of view.

2.2.2.1 HAW

Use the HAW to organize the SRM panel's deliberations into 16 key categories. It is at the panel's discretion to decide which items belong in the HAW. It provides a snapshot of the SRM panel conclusions and will be included in the SRM document for each hazard identified.[3]

Table A.1: HAW

Hazard Description:

1.	2.	3.	4.
Hazard ID	**Hazard Description**	**Cause**	**System State**
Alpha-numeric identifier (under 10 characters)	Any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment	The origin of a hazard	An expression of the various conditions, characterized by quantities or qualities, in which a system can exist

Controls:

5.	6.
Controls	**Control Justification**
Any means currently reducing a hazard's causes or effects	A justification for each control, indicating its effect on the identified hazard's causes or effects

3. All SRM documentation (with the exception of the Program Safety Plan, Operational Safety Assessment, Comparative Safety Assessment, and System Safety Assessment Report) requires the use of a HAW. Worksheets specific to these documents are contained in the Safety Risk Management Guidance for System Acquisitions.

Initial Risk:

7.	8.	9.	10.	11.	12.
Effect	**Severity**	**Severity Rationale**	**Likelihood**	**Likelihood Rationale**	**Initial Risk**
The real or credible harmful outcome that has occurred or can be expected if the hazard occurs in a defined system state	The consequences or impact of a hazard's effect or outcome in terms of degree of loss or harm	Explanation of how severity was determined	The estimated probability or frequency, in quantitative or qualitative terms, of a hazard's effect or outcome	Explanation of how likelihood was determined	The composite of the severity and likelihood of a hazard, considering only controls and documented assumptions for a given system state

Safety Requirements:

13a.	13b.	14a.	14b.
Safety Requirement Description	**Planned for Implementation?**	**Organization Responsible for Implementing Safety Requirement**	**POC**
A planned or proposed means to reduce a hazard's causes or effects	Denotes whether the safety requirement is planned for implementation (yes/no)	The organization's name / routing code	POC's name and telephone number

Predicted Residual Risk:

15a.	15b.
Predicted Residual Risk	**Predicted Residual Risk Rationale**
The risk that is estimated to exist after the safety requirements are implemented or after all avenues of risk mitigation have been explored	If necessary, any additional explanation needed to help the reader understand how the predicted residual risk was determined

Safety Performance Target:

16.
Safety Performance Target
The measurable goals that will be used to verify the predicted residual risk of a hazard

2.2.2.2 Monitoring Plan

Use a monitoring plan table to organize the SRM panel's plan for monitoring the safety performance target and verifying the predicted residual risk for each hazard identified. Information from the monitoring plan will be needed for the SRM document and entry into SMTS.

Table A.2: Monitoring Plan

1.	**Safety Performance Target**	Provide a safety performance target (as documented in the HAW) that can be used to verify the predicted residual risk for the hazard
2.	**Hazard ID(s)**	Provide the hazard ID(s) from the HAW that is associated with this safety performance target

3.	**Initial Risk**	Include the initial risk from the HAW
4.	**Safety Requirements**	Include the means that will be implemented to reduce the hazard's causes or effects from the HAW
5.	**Organization Responsible for Implementing Safety Requirements**	Include information on the responsible organization / POC documented in the HAW
6.	**Predicted Residual Risk**	Include the predicted residual risk from the HAW
7.	**Monitoring POC(s)**	Enter the name and contact information of the person who will be responsible for conducting the monitoring of this safety performance target
8.	**Monitoring Activities**	Describe the tasks that will be led by the monitoring POC to collect and analyze data to verify the predicted residual risk
9.	**Monitoring Start Date**	Enter the date when the monitoring activities should begin
10.	**Reporting Frequency**	Specify how often the monitoring activities will be reported
11.	**Reporting Duration**	Specify the total length of time for the monitoring effort

2.2.3 Factors that Jeopardize SRM Panel Results

Failure to adequately describe the system and scope the NAS change or existing safety issue can negatively affect the fidelity of the SRM process. Change proponents, SRM panel facilitators, and SRM panel members should adhere to the following guidelines to help ensure that SRM panel deliberations are relevant to the NAS change or existing safety issue:

- Sufficiently define the scope.
- Involve relevant stakeholders.
- Identify drivers and constraints.
- Define product boundaries and external interfaces.
- Baseline the scope before writing requirements.

3. Developing SRM Documentation

The change proponent, with assistance from the facilitator or other AJI specialist when/as needed, must select the appropriate SRM documentation type based on the rigor of SRM that was required for addressing the NAS change or existing safety issue and—in some cases—the results of the analysis (i.e., whether hazards were identified). All SRM analyses for NAS changes or existing safety issues must be documented in an SRM Safety Decision, an SRM Document With Hazards **or** an SRM Document Without Hazards. If assistance is needed to determine the appropriate SRM documentation, contact an AJI SCL via the ATO SMS mailbox for assistance; or for SRM guidance regarding local changes, contact the appropriate Service Area Quality Control Group. (See the AJI SRM Pre-Panel webpage for contact information.)

3.1 Documenting an SRM Safety Decision

If the change proponent determines the NAS change does not require high rigor of SRM (i.e., if the change does not require further SRM after the "Describe the System" or "Identify Hazards" phases of the DIAAT process), the SRM Safety Decision serves as the record and explanation for this determination. (See ATO SMS Manual Section 3.3 and its subsections for information on determining the appropriate rigor of SRM and ATO SMS Manual Section 3.4 for a description of the full DIAAT process). Complete SRM Safety Decisions must be uploaded in SMTS.

This SRM Safety Decision must contain the following information:

- Title of the change
- Change proponent organization or facility
- Justification for SRM safety decision
- Current system description
- Description of proposed change
- Change proponent signature attesting to the completeness and validity of the information provided
- Fields applicable for change proponents conducting Two-Phase Local SRM:
  - Confirmation of whether the process identified the potential for hazards
  - Rationale for a safety finding with no potential hazards
  - List of parties who participated in the Two-Phase Local SRM process and can attest to the validity and accuracy of the results
  - Approval signature from appropriate management level attesting to their awareness of the SRM activity and results (See ATO SMS Manual Section 5.1 for information on signature requirements.)
  - Concurrence signature from an SRM expert attesting to the correct application of the SRM process (See ATO SMS Manual Section 5.5 for information on documentation concurrence.)

The SRM Safety Decision may also serve as a record of the determination that a proposed change has no potential to affect ATM/CNS services and thus **is not** a NAS change; however, documentation in such cases is not required. For additional guidance about documenting the SRM Safety Decision, visit the ATO SMS Toolbox for a template or more information.

3.2 Writing an SRM Document[4]

When high rigor of SRM is required for the NAS change (i.e., when the NAS change requires that an SRM panel be convened), an SRM document is used to record the SRM panel attendees’ determinations for NAS changes and existing safety issues. (See ATO SMS Manual Section 3.3 and its subsections for guidance on determining the appropriate rigor of SRM, and ATO SMS Manual Section 3.4 for a description of the full DIAAT process.) The SRM document presents evidence supporting whether the NAS change and/or risk management strategies should be accepted by ATO or FAA management officials from a safety risk perspective. There are two types of SRM documents:

- **Safety Finding With Hazards:** When an SRM panel determines that a NAS change or existing safety issue could introduce hazards or increase safety risk, the panel must complete each phase of the DIAAT process. Typically, this results in new means to reduce risk (i.e., safety requirements) being devised and proposed for implementation. Safety risk and overall safety performance must be monitored after implementation of

4. Refer to the Safety Risk Management Guidance for System Acquisitions for guidance on writing SRM documents for acquisitions.

the NAS change and/or safety requirements to address the identified hazards. This information should be contained in an SRM Document With Hazards.[6]

- **Safety Finding Without Hazards:** When an SRM panel determines that a NAS change will not introduce hazards or increase the safety risk associated with existing hazards, the panel findings are documented in an SRM Document Without Hazards. The SRM document should include a description of the system and NAS change and a rationale explaining why the change does not introduce hazards or increase safety risk.

The change proponent, the SRM panel facilitator, or a designated individual should begin drafting the SRM document immediately after the SRM panel meeting. The draft SRM document should be presented to the SRM panel to verify that the SRM panel members' discussions have been correctly recorded and consensus has been achieved. In the event that an SRM panel member does not concur with a determination made during the risk analysis or risk assessment phases of the process, they are encouraged to submit a dissent in writing. Such dissents are included in the SRM document for evaluation by the risk acceptance official.

The change proponent, the SRM panel facilitator, a designated individual, or the organization responsible for accepting safety risk must enter the SRM document into SMTS.

The following list reflects the applicable sections and criteria for SRM documents:

- Executive Summary
- SRM Document Signatures
- Current System
- Description of Change / Existing Safety Issue
- Rationale for a Safety Finding Without Hazards (if no hazards are identified)
- Hazard Identification and Risk Determination (if hazards are identified)
- Monitoring Plan (if hazards are identified)
- Dissention (when applicable)
- SRM Panel Attendees
- Appendices

For additional guidance about writing either type of document, consider using the SRM document templates available in SMTS and on the ATO SMS Toolbox.

3.2.1 Executive Summary

Use the Executive Summary to provide only the substantive information necessary for decision-makers to understand the current system; NAS change / existing safety issue; and, if applicable, the associated safety risk and proposed ways to address the hazards and safety risk. Provide detailed information and supporting narrative on these items in the body of the SRM document.

Include the following administrative information regarding the SRM document:

- **Title.** Include a clear, concise name of the document with which the document's subject can be easily understood.

6. When addressing existing safety issues, the approach for safety findings with hazards is the most appropriate.

- **Change Proponent Organization.** Provide the organization that is initiating the NAS change or that has taken responsibility for addressing the existing safety issue. Include the organization's name and FAA routing code.
- **Document Type.** Indicate the document type, such as Operations, Second-Level Engineering, etc.

For SRM Documents With Hazards, use the tables below to summarize the hazards identified and proposed means of mitigation/monitoring:

Table A.3: Hazard Summary

Hazard ID	Hazard Description	Initial Risk	Predicted Residual Risk

Table A.4: Safety Requirements

Safety Requirement	Associated Hazard ID(s)	Organization Responsible	POC Signature

Table A.5: Monitoring Plan Summary

Safety Performance Target	Associated Hazard ID

If no hazards are identified, do not include the above tables. Instead, provide a brief rationale for a safety finding without hazards.

3.2.2 SRM Document Signatures

Listed below are the signatures required on the SRM document signature page. For each signatory, include the printed name, signature (handwritten or electronic), organization, and date. Signatures should be obtained and must be listed in the following order: concurrence (when appropriate); approver; risk acceptor; and the Director of Policy and Performance, AJI-3, when necessary.

1. **Concurrence.** Include a concurrence signature from an SRM expert who is well-versed in this SMS Manual and familiar with the terminology and processes therein. This signature is used to represent a technical review of the SRM document and to confirm the rationale used throughout is consistent with the SRM process.
2. **Approval.** Include an approval signature from an official representing the organization responsible for implementing the NAS change (and from the AJI-3 Director, if required). An approver provides a technical and administrative quality control review of the SRM document, its findings, and the identified results.

   Note: The official responsible for the approval signature cannot have been an SRM panel member.
3. **Risk Acceptance.** Include a risk acceptance signature from an appropriate official representing the organization that will be using the safety-assessed NAS equipment, policy, or procedure. This signature indicates confirmation by the official that they

understand the safety risk associated with the NAS change or existing safety issue and that they accept that safety risk into the NAS. Risk acceptance requires that signatures have been obtained for the safety requirements identified in the SRM document and that a comprehensive monitoring plan has been developed and will be followed to verify the predicted residual risk.

The safety requirements signatures from the responsible organization(s) and associated POC(s) are contained within the Executive Summary.

3.2.3 Current System

Provide a detailed description of the hardware/software system, operation, or procedure that constitutes the NAS change or the environment in which the existing safety issue has manifested. Include the following information, when applicable:

- A brief background on what triggered the need for a NAS change or the evaluation of an existing safety issue. If there is an associated SRM document, compliance issue, or high-priority safety issue that necessitated this NAS change, briefly summarize it here, and include the associated reference or documentation as attachments.
- The current hardware or software system or existing procedures/operations and the corresponding (operational) system states.
- The current procedure and its operational environment and, when applicable, a discussion about elements of this issue that make it particularly unique or challenging.
- Equipment or procedures needed to accommodate the implementation of the NAS change.
- Future configuration, system, or procedural changes that might affect the proposed change/procedure or existing safety issue.

3.2.4 Description of Change / Existing Safety Issue

Provide a description of the proposed NAS change or the existing safety issue being addressed. Include the following information, when applicable:

- A description of the proposed NAS change/procedure or existing safety issue and any critical safety parameters that are involved (e.g., prohibited/restricted airspace, noise abatement area, and operational limitations).
- When applicable, discuss the types of verifications that will be performed throughout the development process to review whether the finalized proposed NAS change will be safe, operational, and effective once implemented. Evaluation can consist of simulator modeling, live testing, or a combination thereof.
- A depiction of the proposed NAS change/procedure or existing safety issue (if visual illustration is beneficial).
- Assumptions that make evaluating the NAS change or existing safety issue more manageable or that better scope the change or issue undergoing SRM.
- A summary of the relevant results of any related or preceding safety analyses (i.e., an acquisition program or operational change). Include any references and/or associated documentation mentioned in Section 3.2.10 of this Annex.
- The traceability between the proposed change and the NAS Enterprise Architecture.

3.2.5 Rationale for a Safety Finding Without Hazards (If No Hazards Are Identified)

There may be cases in which, through performing elements of the SRM process (i.e., describing the system / NAS change and identifying hazards), the SRM panel does not identify hazards associated with the implementation of the NAS change, or the SRM panel determines that the NAS change does not increase the current risk level. In such cases, include a detailed rationale that explains how the SRM panel came to that conclusion. When the provisions of this section apply, the SRM document is nearly complete. Follow the guidance for Dissention (when applicable), SRM Panel Attendees, and Appendices, and prepare the SRM document for signatures.

3.2.6 Hazard Identification and Risk Determination (If Hazards Are Identified)

Provide a detailed explanation of each hazard identified. Provide the completed HAW for each hazard (see Section 2.2.2.1 of this annex for instructions on creating a HAW) and the information necessary to support the risk overview in the Executive Summary.

3.2.7 Monitoring Plan (If Hazards Are Identified)

Complete a monitoring plan for each hazard identified (see Section 2.2.2.2 of this annex for instructions on creating a monitoring plan). Provide the completed monitoring plan table for each hazard and the information necessary to support the monitoring overview in the Executive Summary.

3.2.8 Dissention and Opposing Opinions (When Applicable)

The SRM panel process strives for agreement by all panel members with official findings, such as risk ratings. SRM panel member discussions and disagreements that take place while working toward consensus are not dissentions if the SRM panel member ultimately agrees with or can accept the panel's official findings, but such proceedings should be detailed in the body of the SRM document. If a panel member disagrees with the SRM panel's final conclusions, that panel member must provide the nature and summary of the disagreement in writing. Though not required, SMEs may also document their disagreement with a panel's conclusions. Formally documented disagreements from SMEs are recorded as opposing opinions and included in the appendices of (or as attachments to) the SRM document.

SRM panel members and SMEs must submit dissentions / opposing opinions during the SRM document comment adjudication process or, if no comments are received on the SRM document, prior to the signatory process.

3.2.9 SRM Panel Attendees List

Include a table with each SRM panel attendees' name and relevant information including their position, facility, and FAA routing code. Clarify each attendees' role (i.e., facilitation team member, change proponent, SRM panel member, SME, or SRM panel observer).

3.2.10 SRM Document Appendices

Use appendices to include the following, as appropriate:

- Supporting documentation, such as simulations, modeling, and other technical analyses;
- Relevant references; and
- Acronyms, terms, and definitions.

3.3 SMTS

SMTS is the official repository for all completed ATO SRM documents.[7] The change proponent is responsible for ensuring that the SRM document is entered into SMTS before the initiation of monitoring activities, the full implementation of the NAS change, or the achievement of an FAA Acquisition Management System decision point. The change proponent may record the information directly, designate a responsible individual, or work with the SRM panel facilitator or organization responsible for accepting safety risk to enter the SRM document into SMTS. See the Safety Risk Management Guidance for System Acquisitions for a more detailed description of mandatory entry requirements for acquisition programs.

3.3.1 Implementation Dates in SMTS

Once the SRM document has been completed and all required signatures have been obtained, the change proponent is responsible for providing a monitoring start date (i.e., the date after all safety requirements are implemented). This date must be entered into SMTS to trigger the automated email notification process for the monitoring plan.

4. Special SRM Considerations for Waiver Renewals and Approvals

4.1 Overview

This section provides guidance for SRM considerations specific to waiver or authorization renewals and approvals.

4.2 Documentation, Review, and Approval Process for Waivers to Separation Standards

A waiver to separation standards can result in aircraft being allowed closer than approved separation from terrain, obstacles on the surface of the earth, airspace, or other aircraft. FAA Order JO 7110.65, *Air Traffic Control*, lists the requirements that pertain to separation standards.

Any new waiver or authorization request or waiver/authorization renewal request that pertains to separation standards requires a new SRM document or an SRM document on file that is developed in accordance with the ATO SMS Manual. The SRM document should include a quantitative analysis (e.g., scientific study, Flight Standards Service report, detailed modeling, or Monte Carlo simulation) to support the information provided.

4.2.1 Initiate the Request for a New Waiver or Waiver Renewal

Waivers must be kept to a minimum as they contribute to a nonstandard NAS. Before developing or renewing a waiver, coordinate with the appropriate Service Area and Service Unit to obtain their commitment to the effort. The Service Unit will coordinate with AJI to determine whether additional information is warranted to support the request and SRM document.

4.2.2 Waiver Development Guidance: Identify Appropriate Hazards

Most paragraphs in FAA and ATO orders mitigate a potential safety hazard. Attempt to identify the hazard that the relevant order intends to mitigate to determine the appropriate hazard(s) to address in the SRM document. If the waiver request is intended to reduce safety risk, then ensure there is sufficient justification in the SRM document, and show the waived procedures as a means to reduce risk in the HAW.

4.2.3 Relationship between the Waiver Request and the SRM Document

All of the following waiver requirements should be covered in the SRM document:

7. A completed SRM document includes all required signatures (both ink and digital signatures are accepted).

- The “Affected Directive” and “Operations Authorized” sections of the waiver should match the “Description of Change” section of the SRM document.
- The “Special Provisions, Conditions, and Limitations” section of the waiver should flow out of the HAW section of the SRM document, specifically from the controls, system states, and/or the safety requirements.
- Remember to include any new safety requirements in the SRM document.

4.2.4 Waiver Renewals

Waivers must be renewed in accordance with existing ATO guidance as prescribed in FAA Order JO 7210.3, *Facility Operation and Administration*. When submitting a waiver renewal request, read the current SRM document to determine whether any updates are necessary. Keep in mind that an SRM document must be updated to reflect the current operational environment. All required means to reduce risk (including the publication of information and any refresher training requirements, as delineated in the original SRM document) must be in place.

For each waiver renewal request:

- Determine whether the level of safety risk that was introduced with the initial waiver remains acceptable,
- Use the safety performance monitoring results per the monitoring plan to allow the responsible organization to determine whether the waiver is working as intended, and
- Determine whether the provisions of the waiver have matured sufficiently that they should be made available to all others in the NAS through inclusion in FAA Order JO 7110.65.

Before submitting a waiver renewal request, ensure the monitoring information pertaining to the existing waiver is up to date in SMTS. All proposed modifications to any provision of the current waiver will require a new waiver to be developed with a new SRM document.

4.2.5 Waiver Approval

All new waivers and waiver renewal requests will be approved by AJI. AJI will coordinate the approved waiver with AOV, if necessary. Ensure that new waivers and information pertaining to waiver renewals are entered in SMTS.