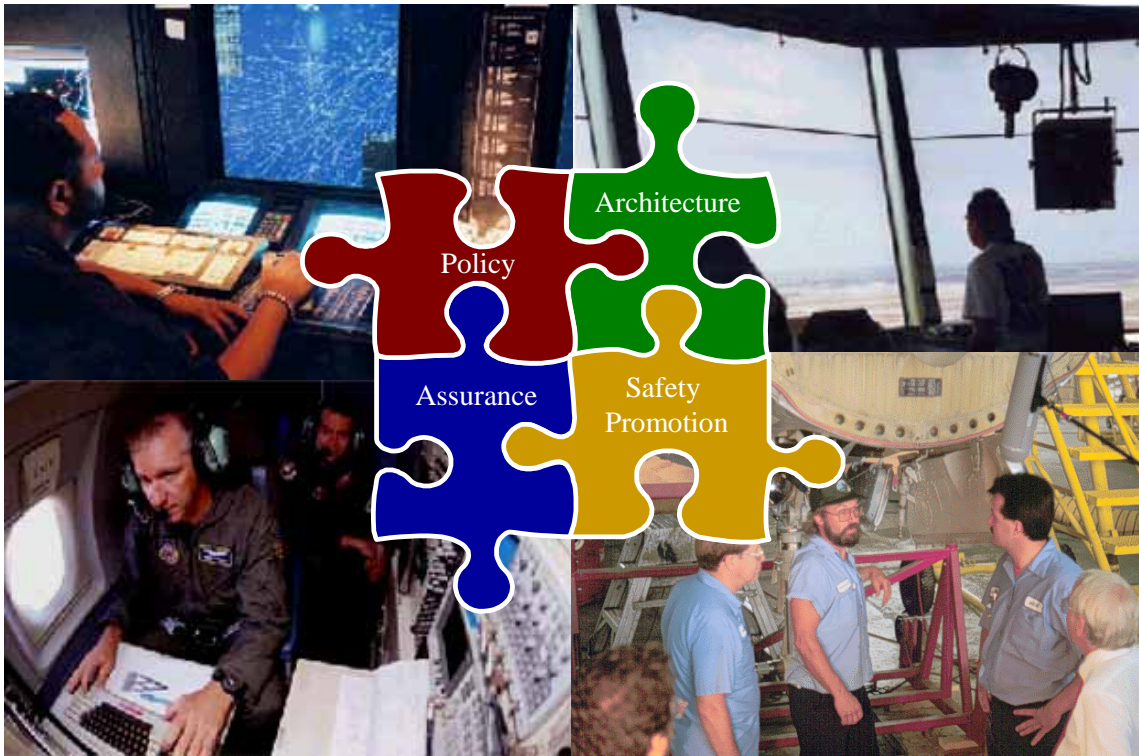


Federal Aviation Administration Safety Management System Manual



Version 1.1

May 21, 2004

Table of Contents

Foreword.....	i
Introduction to the Safety Management System.....	i
Chapter 1 – Safety Management System Overview.....	1
Chapter 2 – SMS Requirements	8
Chapter 3 – Applicability of Safety Risk Management.....	15
Chapter 4 – Safety Risk Management Guidance	21
Chapter 5 – Safety Risk Management Documentation: Development and Approval.....	55
Chapter 6 – Safety Assurance and Evaluation.....	60
Chapter 7 – Safety Data Tracking and Analysis.....	68
Chapter 8 – SMS Responsibilities and Accountabilities	77
Chapter 9 – SMS Training Standards	79
Chapter 10 – Safety Culture	83
Chapter 11 – Safety Oversight.....	87
Appendix A – References to FAA Documents Related to SMS Requirements.....	A-1
Appendix B – Hazard Identification Tools.....	B-1
Appendix C – SRM and Changes to Air Traffic Control Procedures	C-1
Appendix D – Documenting Safety Risk Management	D-1
Appendix E – Glossary of Terms.....	E-1
Appendix F – Acronyms/Abbreviations	F-1

Foreword

The United States has one of the safest and most complex aviation systems in the world, providing safe air travel 24 hours a day, 365 days a year. Each day the National Airspace System (NAS) handles more than 35,000 airline operations. Federal Aviation Administration (FAA) management plays a crucial role in the provision of safe air traffic control (ATC) and navigation services as cross-organizational changes to the NAS are more complex and interrelated.

The FAA assigns the highest priority to maintaining safety. An important step towards the future is the implementation of an integrated Safety Management System (SMS). The SMS integrates current FAA safety-related operational policies, processes, and procedures, as well as introduces new elements necessary for a systems approach to managing the safety risk of providing ATC and navigation services.

This manual provides high-level structure, procedures, and responsibilities regarding the functioning of the SMS. It provides a framework for identifying and analyzing safety risk to appropriately mitigate and manage it as the FAA continues to maintain and improve ATC and navigation services. While the manual focuses on clarifying safety management processes of those organizations within the Air Traffic Organization (ATO), it is important to note that this manual is applicable to all FAA organizations that promote and approve changes that affect the provision of ATC and navigation services.

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

Marion C. Blakey
Administrator

Introduction to the Safety Management System

The Safety Management System (SMS) provides a systematic and integrated method for managing safety of air traffic control (ATC) and navigation services in the National Airspace System (NAS). This manual documents the SMS, building on existing Federal Aviation Administration (FAA) safety management capabilities. Major elements of the SMS include:

- **Policy:** The SMS requirements, responsibilities, and accountabilities for system functions
- **Architecture:** The processes, procedures, and practices used to assess changes to the NAS for safety risk and document those changes
- **Assurance:** The processes used to assure safety of the NAS, including evaluations and inspections, as well as data tracking and analysis
- **Safety Promotion:** Communication and dissemination of safety information to strengthen the safety culture and support integration of the SMS into operations

The manual provides guidance and procedures for managing the safety of the NAS. Safety management roles are defined, as are the processes and principles of safety risk management (SRM). The manual provides guidance and procedures, and clarifies responsibilities for documenting SRM activities. The SMS addresses the need for the continued collection and analysis of safety data to identify trends regarding ATC and navigation services. The manual provides tools, procedures, and processes for identifying, analyzing, mitigating, and tracking safety hazards – leading to a safer NAS.

The SMS applies to all FAA employees, managers, and contractors who are either directly or indirectly involved in the provision of ATC and navigation services. Documentation such as safety risk management documents (SRMDs), safety incident reports, and safety inspection and evaluation reports provide managers with needed information regarding safety hazards and risks associated with systems (hardware and software), procedures, and airspace designs.

In many instances, formal SRM is already part of engineering, acquisition, and management processes, and safety data monitoring is an every day activity in many organizations. In these cases, the SMS integrates existing safety management processes, documentation, and daily activities. As the SMS matures, some safety-related processes may require re-engineering, and others may need to be developed.

Roles, processes, procedures, and guidance documentation will continue to evolve as the SMS matures. As the SMS is implemented, supporting documents to the manual will be developed to address specific aspects of the SMS, as well as to focus on specific organizations and/or functions and their safety management processes. The manual is an umbrella document, related to many current and future orders and regulations, which over time will be further developed and linked.

As the SMS is implemented, organizations will integrate SRM principles and processes into their national, regional, and local activities and processes. The ATO Safety Service Unit will facilitate SMS implementation and will be responsible for managing SMS processes and documents, facilitating SMS training, providing safety risk management expertise, when necessary, auditing SRM processes, and evaluating the SMS.

In the “end state,” the SMS will be an integrated collection of processes, procedures, policies, and programs used to assess, define, and manage the safety risk in the provision of ATC and navigation services. It will ensure a formalized and proactive approach to system safety through SRM.

Chapter 1 – Safety Management System Overview

1.1 *What is the purpose of this document?*

This document describes the Federal Aviation Administration's (FAA) Safety Management System (SMS), a key element of the evolution and advancement of safety in the United States National Airspace System (NAS). The SMS integrates existing FAA operational policies, processes, and procedures, as well as introduces new elements necessary for a systems approach to managing the safety risk of providing air traffic control (ATC) and navigation services.

The SMS provides a common framework to assess safety risks of changes to the NAS. The SMS addresses all aspects of ATC and navigation services, including airspace changes, air traffic procedures and standards, airport procedures and standards, and new and modified equipment (hardware and software). The SMS facilitates cross-functional safety risk management (SRM) among the ATC service providers and ensures intra-agency stakeholder participation in solving the safety challenges of an increasingly complex NAS. The SMS helps reduce the number of isolated safety decisions, which at times, result in wasted time and resources.

In addition, the SMS includes processes to collect and analyze safety data, conduct safety reviews and evaluations, and continuously monitor data to ensure NAS safety.

The SMS is expected to evolve as a result of lessons learned through the application of SMS tools and concepts, changing technologies, advances in aviation operations, and improved techniques for managing risk.

1.2 *How is this document organized?*

This manual describes the functions, components, and principles of the SMS. In general, each chapter covers one of the components of the SMS. Given its complexity, SRM comprises three chapters.

1.3 *Why an SMS?*

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

In 2000, the FAA Administrator instructed an FAA team to study SMSs. Shortly thereafter, management concluded that the design,

development, and implementation of an SMS are important next steps for aviation safety.

In addition, in November 2001, the International Civil Aviation Organization (ICAO) amended Annex 11 to the Convention, *Air Traffic Services*,¹ to require that member states establish an SMS for the provision of air traffic services. The SMS requirements described in Annex 11 are further detailed in ICAO Document 4444, *Procedures for Air Navigation Services, Air Traffic Management (PANS-ATM)*.² The SMS documented in this manual meets ICAO SMS requirements.

1.4 *Who is affected?*

The provision of ATC or navigation services requires collaboration among the Air Traffic Organization (ATO), Regulation and Certification (AVR), Airports (ARP), and any other organization or Line of Business (LOB) that promotes and approves NAS changes that affect the safe delivery of ATC and navigation services.

The SMS applies to all FAA employees, managers, and contractors who are either directly or indirectly involved in the provision of ATC or navigation services.

1.5 *What is the scope of the SMS?*

The SMS can only provide a means of controlling those safety hazards that originate within the NAS, or in which some element of the NAS is a contributory factor. As an example of the latter, the SMS cannot directly address the causes of an in-flight emergency due to an aircraft system malfunction. However, it is important that the ATC procedures for handling an in-flight emergency do not contribute to the possibility of the emergency resulting in an accident.

The SMS does not cover occupational safety (e.g., Occupational Safety and Health Administration (OSHA)) or information security, which are already addressed by other programs and processes. Instead, the SMS focuses on the safe provision of ATC and navigation services

1.6 *What is the FAA's safety mission?*

The SMS reinforces the FAA's mission to provide a safe, secure, and efficient global aerospace system. "Safety is the FAA's

¹ ICAO Annex 11 to the Convention on International Civil Aviation, Air Traffic Services, Thirteenth Edition – July 2001, Section 2.26.

² ICAO Document 4444 (ATM/501), Procedures for Air Navigation Services, Air Traffic Management, Fourteenth Edition – 2001, Chapter 2.

primary mission."³ Safety is the principal consideration of all FAA activities.

1.7 *What is included in an SMS?*

The SMS is an integrated collection of processes, procedures, policies, and programs that assess, define, and manage the safety risk in the provision of ATC and navigation services.

As depicted in Figure 1.1, the SMS can be broken down into the following components:

- **Policy:** The SMS requirements, responsibilities, and accountabilities for system functions
- **Architecture:** The processes, procedures, and practices used to assess changes to the NAS for safety risk and documentation of those changes
- **Assurance:** The processes used to ensure safety of the NAS, including evaluations and inspections, as well as data tracking and analysis
- **Safety Promotion:** Communication and dissemination of safety information to strengthen the safety culture and support integration of the SMS into operations

The SMS provides a formalized and proactive approach to system safety through SRM and continuous safety data monitoring. Before implementing a change in the NAS, the safety impact is evaluated. If the change is safety significant (i.e. a change that could reasonably impact NAS safety), a risk assessment is performed to identify the effect of the change on NAS safety.⁴ The types of changes that require safety risk assessments, as well as the requirements, processes and procedures, and outcomes and documentation requirements of safety risk assessments are described further in Chapter 4, *Safety Risk Management Guidance*, and Chapter 5, *Safety Risk Management Documentation: Development and Approval*. As described in Chapter 4, the depth and complexity of the safety risk assessment are tailored to the scope and degree of safety impact of the change. The SRM process ensures that safety related changes are documented, problems and issues are tracked to conclusion, and ongoing performance is monitored.

Monitoring includes safety assurance and evaluation programs to ensure program compliance and process integrity, as well as the

³ Federal Aviation Administration Flight Plan 2004–2008 (at <http://www1.faa.gov/AboutFAA/FlightPlan.cfm>).

⁴ A key building block of the SMS is the safety risk management program established by FAA Order 8040.4, *Safety Risk Management*.

collection and analysis of safety data. Safety data are collected from a wide range of sources, and the data and results of assurance and evaluations are analyzed for adverse trends. Safety assurance and evaluation are further described in Chapter 6, *Safety Assurance and Evaluation*. For more information on the collection and analysis of safety data, refer to Chapter 7, *Safety Data Tracking and Analysis*.

In addition to the evaluations, audits, and inspections, the ATO Safety Service Unit evaluates the overall effectiveness of the SMS.

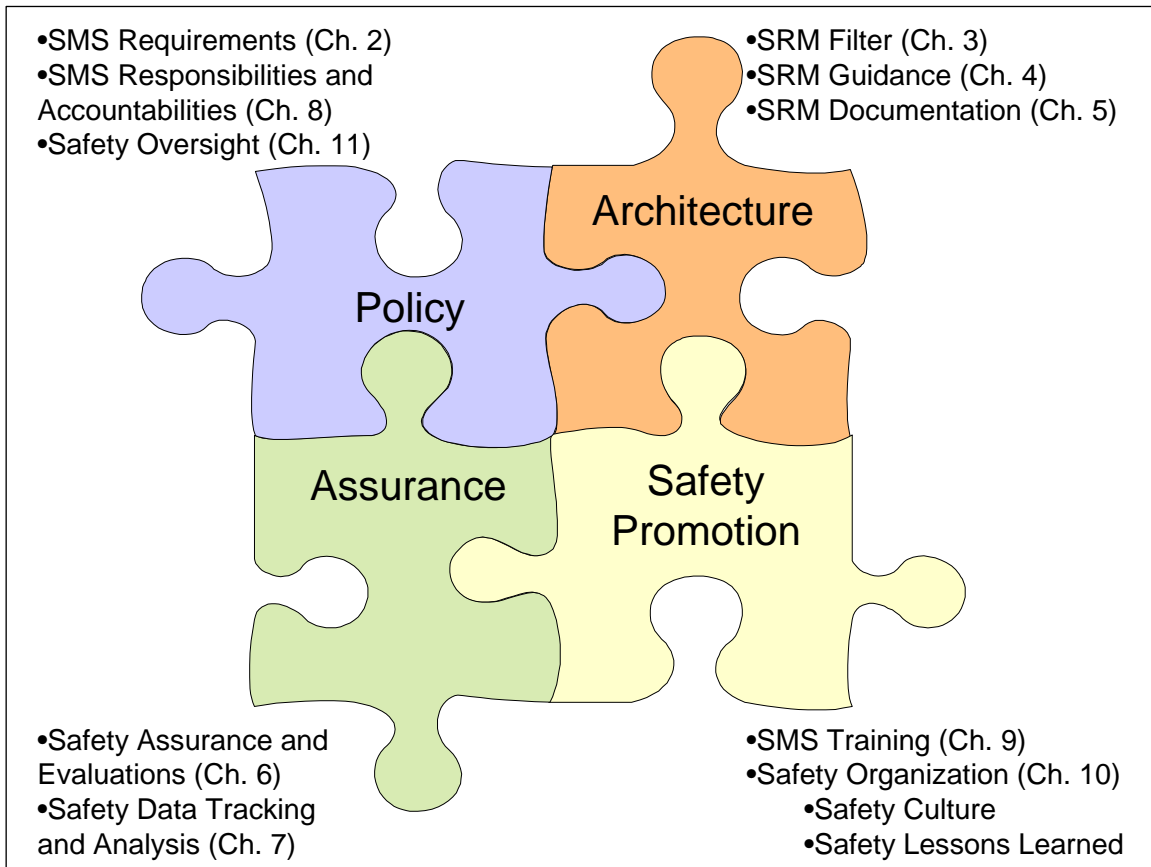


Figure 1.1 - Safety Management System Components

1.8 *What are the products of the SMS?*

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

1.9 *Who is responsible and accountable for safety of the NAS?*

Safety is an inherent component in the delivery of FAA services. FAA culture enforces the understanding that safety is the most important aspect of any activity or decision. All FAA employees, managers, and contractors who are either directly or indirectly involved in the provision of ATC or navigation services are accountable for safety in their areas of responsibility. The outcomes and products of the SMS provide input (from a safety perspective) to allow informed and efficient decisions within management's purview. Clear lines of responsibility and accountability (as defined in Chapter 8, *SMS Responsibilities and Accountabilities*) are necessary to foster a safety culture in which all employees feel personally responsible for the safety aspects under their control.

1.10 *What is a safety culture?*

In this context, a safety culture refers to the personal dedication and accountability of individuals engaged in any activity that has a bearing on the safe provision of air traffic services. It is a pervasive type of safety thinking that promotes an inherently questioning attitude, resistance to complacency, a commitment to excellence, and the fostering of both personal accountability and corporate self-regulation in safety matters.

Safety culture then is both attitudinal as well as structural, relating to both individuals and organizations. It concerns the requirement to not only actively identify safety issues but to respond with appropriate action. Safety culture relates to such intangibles as personal attitudes and the style of the organization. It is therefore difficult to measure, especially when the principal criterion for measuring safety is the absence of accidents and incidents. Yet, personal attitudes and corporate style can enable or facilitate the unsafe acts and conditions that are the precursors to accidents and incidents.

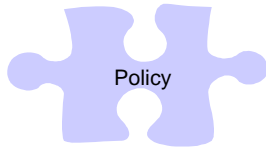
Safety culture goes beyond mechanistic adherence to procedures. It requires that all duties important to safety be carried out correctly, with alertness, due thought and full knowledge, sound judgment, and a proper sense of accountability.

1.11 *How does the SMS relate to the FAA's mission?*

The SMS supports the FAA's mission by reinforcing the principle that safety is the main consideration in any activity the FAA undertakes. The primary goal in the delivery of air traffic services is to ensure the safety of flight. The SMS provides safety information and methodologies on which to base decisions and actions.

- 1.12 *What is the safety objective of an SMS?*
- The objective of the SMS is to meet FAA safety goals, which support the FAA's core mission to ensure the safety of the flying public.
-
- 1.13 *What is the ATO Safety Service Unit, and what does it do?*
- A key component of the SMS is the ATO Safety Service Unit. Led by the Vice President (VP) for Safety, this office has several important functions regarding the SMS and NAS safety. These include:
- advocating a safety culture
 - leading implementation of the SMS across the FAA
 - managing and updating SMS processes and supporting documentation (e.g., FAA SMS Manual and guidance materials)
 - facilitating SMS training (including SRM training)
 - reviewing and providing input on safety risk assessments
 - auditing SRM and assurance processes and outputs
 - facilitating coordination of SRM and controls with cross-organizational impacts
 - monitoring the safety of the NAS through data analysis
 - reviewing existing safety data reports and developing new reports as necessary to further describe the status of the NAS in regards to safety and inform decision-makers
 - using the outputs of existing operational quality assurance functions and, where necessary, tracking safety critical issues to conclusion
 - collecting/consolidating and analyzing data on NAS changes
 - advising FAA leadership on safety related issues
 - conducting strategic planning for SMS
 - collaborating (internationally) with other providers of air traffic services to share lessons learned (including specific processes and training), as well as to ensure harmonization of international SMS efforts
 - acting as primary ATO interface with Air Traffic Safety Oversight Service (AOV)
-
- 1.14 *What is the AOV, and what does it do?*
- The FAA Administrator delegated authority to the Associate Administrator for Regulation and Certification to oversee the safety of the ATO. AOV is the organization within AVR that carries out that function. AOV's authority is documented in the Air Traffic Safety Oversight Service Order, which describes AOV and ATO roles and responsibilities regarding NAS safety. ATO service units must comply with the requirements described in the oversight order in addition to SMS requirements in this manual.

AOV's role and function are discussed in more detail in Chapter 11, *Safety Oversight*.



Chapter 2 – SMS Requirements

2.1 *What is the SMS?*

The SMS is an integrated collection of processes, procedures, policies, and programs used to assess, define, and manage the safety risk in the provision of ATC and navigation services. It ensures a formalized and proactive approach to system safety through safety risk management.

The SMS implements the FAA's safety policy (as described in its regulations, orders, directives, manuals, and guidance materials) and defines how the Agency manages safety as an integral part of the provision of service. The SMS also defines the FAA's safety architecture (i.e., processes, procedures, and practices), safety assurance, and safety promotion activities. An integrated SMS facilitates cross-organizational safety risk management (SRM) and provides means and methods for documenting safety management decision-making.

2.2 *What are the fundamental activities and programs of the SMS?*

The SMS is comprised of the following activities and programs:

Safety Risk Management (SRM):

- hazard identification
- safety risk assessments
- hazard tracking and risk mitigation
- monitoring to assess effectiveness of the mitigation strategies

Documentation of SMS Outcomes:

- safety risk management document (SRMD)
- safety data analysis reports
- documentation of safety reviews and evaluations

Safety Assurance and Measurement:

- safety reviews and evaluations
- collection and analysis of safety data
- mechanisms for identifying and implementing safety enhancing measures
- review and monitoring of SRM and assurance processes
- assessing the effectiveness of the SMS in improving NAS safety

Safety Promotion:

- training
- sharing safety data
- dissemination of lessons learned

Many relevant activities pre-date the SMS and are, therefore, detailed in numerous other FAA documents, orders, and processes. To minimize duplication of effort, those documents are referenced throughout this manual. In addition, a matrix listing many of the related documents is in Appendix A.

2.3 What is SRM?

The SMS ensures a formalized and proactive approach to system safety through SRM. Safety risk assessments are developed for changes with safety impacts to identify the effect on NAS safety.

The types of changes that require safety risk assessments, as well as the requirements, processes and procedures, and outcomes and documentation requirements of safety risk assessments are further described in Chapter 3, *Applicability of Safety Risk Management*, Chapter 4, *Safety Risk Management Guidance*, and Chapter 5, *Safety Risk Management Documentation: Development and Approval*.

Chapter 3 describes the decision process to determine what is subject to SRM. Chapter 4 describes the depth and complexity of the safety risk assessment, and how it is tailored to the scope and degree of safety impact of the change. Chapter 5 describes documentation and approval of safety risk assessments.

The SRM process ensures that:

- safety related changes are documented
- risk is assessed and analyzed
- unacceptable risk is mitigated
- hazards are identified and tracked to resolution
- the effectiveness of the risk mitigation strategies is assessed
- the performance of the change is monitored throughout its lifecycle

All relevant factors are considered when conducting a safety risk assessment, including:

- types of aircraft and their performance characteristics, including aircraft navigation capabilities and navigation performance
- systems and/or subsystems intended function and flight or ground environment in which the system is to perform that function
- traffic density and distribution
- airspace complexity, route structure, and classification of the airspace

- airport layout, including runway configurations, runway lengths, and taxiway configurations
- type of air-ground communications and time parameters for communication dialogues, including controller intervention capability
- type and capabilities of surveillance and automation systems, and the availability of systems providing controller support and alert functions
- human factors issues⁵
- any significant local or regional weather phenomena

Figure 2.1 provides an overview of SRM and the NAS.

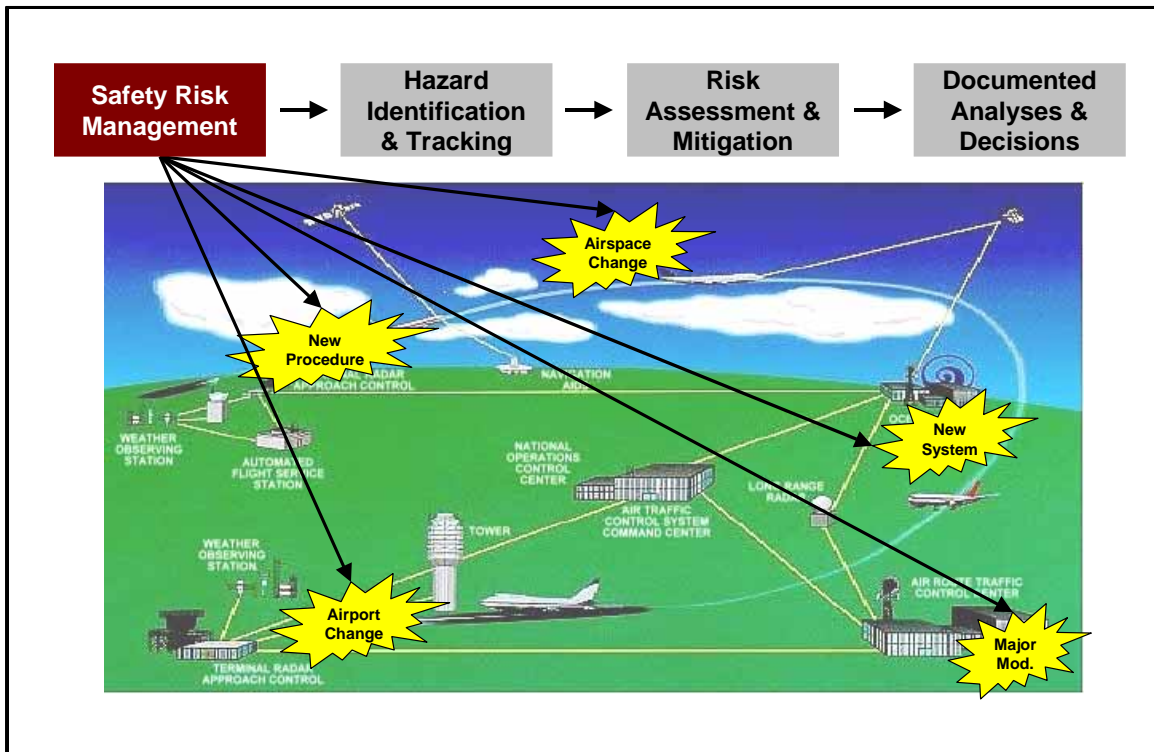


Figure 2.1 - Safety Risk Management and the NAS

2.4 *What is the output of the safety risk assessment?*

The findings of the safety risk assessment are documented in an SRMD. At a minimum, the SRMD documents the change and the findings of the safety risk assessment, and is signed by the appropriate authority effectively implementing the change. The

⁵ For more information regarding the role of human factors in evolving environments, refer to: FAA/NASA Human Factors for Evolving Environments: Human Factors Attributes and Technology Readiness Levels (at <http://www.hf.faa.gov/docs/508/docs/TRL.doc>).

SRMD is further detailed in Chapter 5, *Safety Risk Management Documentation: Development and Approval*.

2.5 *What is assessed when conducting a safety review and evaluation?*

Where applicable, safety reviews are conducted in accordance with FAA Orders. For example, orders that pertain to evaluations include: Order 7010.1, *Air Traffic Evaluations*; 7210.56, *Air Traffic Quality Assurance*; 6000.15, *General Maintenance Handbook for Airway Facilities*; 6040.6, *Airway Facilities NAS Technical Evaluation Program*; 6000.30, *NAS Maintenance Policy*; 3400.3, *United States Standard Flight Inspection Manual*. At a minimum, the reviews must assess:

The documentation to ensure that:

- operations manuals, unit instructions, and ATC coordination procedures are complete, concise, and current
- route structure is designed for minimal controller intervention and inter- and intra-unit coordination
- the separation minima used in the airspace, including the airport, are appropriate, and all the provisions applicable to those minima are being performed
- where applicable, provision is made for adequate visual or radar observation of the maneuvering area, and procedures and measures aimed at minimizing the potential for inadvertent runway incursions are in place
- appropriate procedures for low visibility airport operations are in place and enforced
- traffic volumes and associated controller workloads do not exceed defined safe levels, and procedures are in place for regulating traffic volumes whenever necessary
- procedures to be applied in the event of failures or degradations of air traffic service systems, including communications, navigation, and surveillance systems, are practicable and provide for safe use of the airspace
- procedures for reporting incidents and other safety-related occurrences are implemented
- the reporting of incidents is encouraged; such reports are reviewed to identify the need for corrective action

The operational and technical issues to ensure that:

- the environmental working conditions meet established levels for temperature, humidity, ventilation, noise, and ambient lighting, and do not adversely affect controller performance
- automation systems generate and display flight plan, control, and coordination data in a timely, accurate, and

easily recognizable manner, in accordance with human factors principles

- equipment, including input and output devices for automation systems, is designed and positioned in the working position in accordance with ergonomic principles
- detailed records of systems and equipment serviceability are retained and periodically reviewed
- communications, navigation, surveillance, and other safety significant systems and equipment:
 - a. are tested for normal operations on a routine basis
 - b. perform their intended function(s)
 - c. do not adversely impact other systems in the NAS
 - d. meet the required level of reliability and availability as defined by the appropriate authority
 - e. provide for the timely and appropriate detection and warning of system failures and degradations
 - f. include documentation on the consequences of system, subsystem, and equipment failures and degradations
 - g. include measures to control the probability of failures and degradations
 - h. include adequate back-up facilities and/or procedures in the event of a system failure or degradation

The certification and training to ensure that:

- controllers are adequately trained and properly certified with valid ratings
- controller competency is maintained by adequate and appropriate refresher training, including the handling of aircraft emergencies and operations under conditions with failed and degraded facilities and systems
- when the ATC unit or control sector is staffed by teams, controllers are provided relevant and adequate training in order to ensure efficient teamwork
- implementation of new or amended procedures, and new or modified automation, communications, surveillance, and other safety significant systems and equipment is preceded by appropriate training, instruction, and equipment certification procedures
- controller competency in the English language is satisfactory in relation to providing air traffic services to international air traffic
- standard phraseology is used

For further detail concerning safety assurance and evaluation, refer to Chapter 6, *Safety Assurance and Evaluation*.

2.6 *What is the output of a safety review and evaluation?*

The evaluator documents results of safety reviews and evaluations. The results are provided to the manager of the unit or facility that was reviewed, as well as his or her superior, and are filed with the ATO Safety Service Unit.

2.7 *How is safety data used?*

Data for use in safety monitoring should be collected from as wide a range of sources as possible, as the safety-related consequences of particular procedures or automated systems may not be realized until after an incident has occurred.

The SMS uses a formal incident reporting system for employees to facilitate the collection of information on actual or potential safety hazards or deficiencies related to the provision of air traffic services, including route structures, procedures, communications, navigation, and surveillance systems, and other safety significant systems and equipment, as well as controller workloads. All relevant safety data, including those metrics identified by the FAA safety goals and objectives in Agency strategic and business plans, are tracked, and used to produce the safety reports described below. This information is shared across the FAA.

2.8 *What are the outputs of safety data analysis?*

The outputs of the safety data analysis are reports concerning the operation of air traffic services prepared by the ATO Safety Service Unit, including:

- reports regarding air traffic incidents leading to the detection of adverse trends in the number and types of incidents that occur
- reports concerning the availability of facilities and systems, such as failures and degradations of communications, surveillance, and other safety significant systems and equipment to detect adverse trends that can affect safety

The reports are provided to the appropriate management official with authority to correct identified issues.

For further detail on safety data collection and analysis, refer to Chapter 7, *Safety Data Tracking and Analysis*.

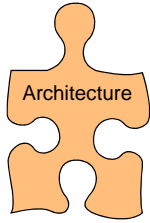
2.9 *What happens to identified risk?*

Whether identified through a safety management activity or by any other means (e.g. thru verification, operational use, etc.), any hazard related to the provision of air traffic services within an

airspace or at an airport (including equipment and equipment components) is assessed and classified for its risk acceptability. Appropriate measures are implemented to eliminate the risk or reduce the risk to an acceptable level. Once implemented, and throughout the lifecycle, the corrective measure's effectiveness in eliminating or mitigating the risk is evaluated.

2.10 *Will safety lessons learned be shared?*

Lessons learned from safety occurrence, incident, and accident investigations, as well as any other activities, whether part of the SMS or not, are shared throughout the FAA to promote SMS maturation and increase the safety of the NAS. Some of the methods for sharing lessons learned include reports, SRMDs, and training. It is expected that sharing of lessons learned will lead to the identification of unacceptable hazards and result in the implementation of steps to mitigate the hazard, making the NAS safer.



Chapter 3 – Applicability of Safety Risk Management

3.1 What is evaluated for safety risk?

All safety significant, new and modified systems, procedures, and operations are evaluated for safety risk. It is management's responsibility to decide if the impact on safety is such that SRM is required.

At a minimum, the safety risk of the following general changes is evaluated and managed in accordance with the SMS, following the SRM process documented in Chapter 4, *Safety Risk Management Guidance*.⁶

- Safety significant airspace changes, including:
 - i. reorganization of air traffic services route structure
 - j. resectorization of an airspace
- Safety significant changes to air traffic services procedures and standards, including:
 - k. reduced separation minima applied to airspace
 - l. new operating procedures, including departure, arrival, and approach procedures
 - m. waivers to existing procedures, requirements, or standards
- Safety significant changes to airport procedures and standards, including:
 - n. reduced separation minima applied at an airport
 - o. physical changes to airport runways, taxiways, or the airport operations area
- The introduction of new safety significant equipment, systems (hardware and software), or facilities used in the provision of air traffic services
- Safety significant modifications to critical equipment, systems (hardware and software), or facilities used in the provision of air traffic services

Since established operations, procedures, and performance of routine maintenance pre-date the implementation of the SMS, they were not evaluated using the SRM processes described in this document. However, they were evaluated during initial design and development (prior to implementation) using the processes that existed at that time and are deemed to be safe based on the FAA's

⁶ This list of safety significant changes was adapted from the list provided in ICAO Document 4444 (ATM/501) *Procedures for Air Navigation Services, Air Traffic Management*, Fourteenth Edition – 2001, Chapter 2. Note: this is not a complete list.

exemplary safety record. SRM described in this manual is used when new or changed items are implemented. For example, a formal safety risk assessment is not necessary when procedurally changing runway direction due to wind changes because this change is predicated on existing standards and procedures. However, one would be conducted during planning and implementation of changes to those existing procedures.

As the SMS is implemented, each Service Unit and/or organization develops or formalizes already existing SRM processes that address its own aspects of providing ATC and navigation services. The NAS changes that prompt the implementation of SRM vary for each of organization.

3.2 *Who decides if a change should follow the SRM process?*

When a system change is proposed, managers decide if SRM is required. SRM is always required if the specific type of change is one that requires approval or acceptance by either AOV or the ATO Safety Service Unit (refer to Sections 5.7, 5.8, 11.5, or 11.6 for types of changes requiring approval or acceptance). Figure 3.1 describes the general process to follow to decide if SRM is required for those changes that are not listed in the sections referenced above.

The following items are considered when determining whether to apply SRM:

- If the change affects the NAS
- If the NAS is affected, then the proponent of the change must determine if the change would reasonably affect NAS safety
- It is appropriate for the decision-maker to use experiential knowledge/judgment to determine if SRM is required
- If at any point it is determined that a safety analysis is not necessary, the decision is documented
- If an analysis is required, the SRM process is followed and documented

Management also decides what level of detail and complexity of an assessment is necessary for the proposed change. It is worthy of note that all decisions made regarding whether SRM is required, must be documented and are auditable by the ATO Safety Service Unit and/or AOV.

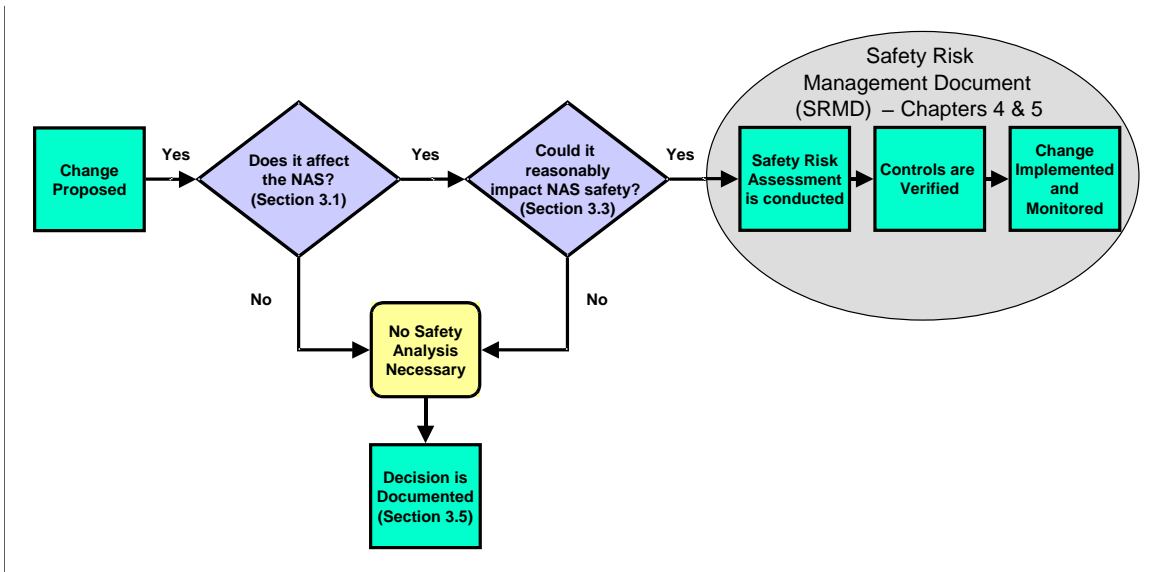


Figure 3.1 - SRM Decision Process

3.3 *What guidance is provided to help determine whether SRM is required?*

SMS training provides a foundation for these types of decisions. In addition, decision-makers' experience is a powerful tool to be used in determining the safety impact of a proposed change. SRM processes are utilized for all safety significant changes to the NAS.

When determining if SRM is required, a fundamental question is asked: does the change impact NAS safety? If the answer is yes, SRM is necessary. Additional questions that need to be asked include:

- Does the change affect pilot and controller interaction?
- Does the change affect existing controller processes or procedures?
- Does the change represent a change in operations?
- Does the change modify the form, fit, and/or function of a critical or essential NAS system?

The basis for initiating the SRM process differs for each organization. The level at which SRM is conducted will also vary by organization and/or proponent, as well as by the type change.

In some cases, SRM is carried out at the national level for major system acquisitions. In other cases, SRM is performed at the regional or local levels to address proposed changes. Figure 3.2 provides examples of changes in the categories listed in Section 3.1.

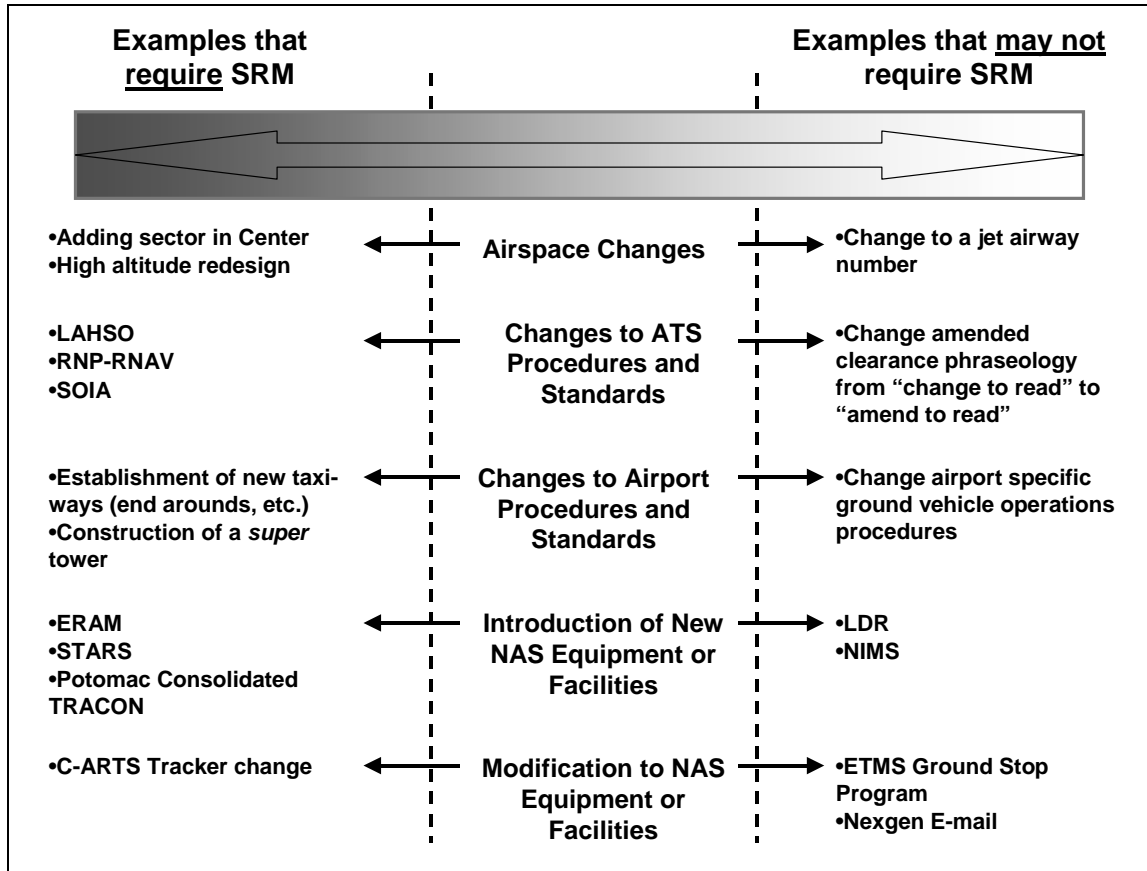


Figure 3.2 - Spectrum of NAS Change Examples

3.4 *How in depth does the analysis have to be?*

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

- The size and complexity of the change under consideration. A larger and more complex change may also require a larger and more complex analysis.
- The breadth of a change. SRM scope can be expected to increase if the change spans more than one organization or LOB.
- The type of change. Technical changes tend to require more analysis than non-technical changes.

For more information regarding the appropriate SRM scope and scale, refer to Section 4.23.

3.5 *What documentation is required?*

The SMS provides a framework for documenting safety management decisions related to proposed changes to the NAS, regardless of whether or not an SRMD is developed.

If a determination is made that the proposed change does not require SRM, a written statement including the decision and supporting argument is signed by the manager and kept on file for a period equivalent to the lifecycle of the system or change.

If SRM is required, SRM processes are followed, and an SRMD matching the type and complexity of the change is developed. More information on SRM and SRMD is included in Chapter 4, *Safety Risk Management Guidance*, and Chapter 5, *Safety Risk Management Documentation: Development and Approval*, respectively.

In addition, each organization maintains an updated list of proposed NAS changes within its purview and the related outcome. Table 3.1 illustrates the format of the tracking matrix and the information to be recorded.

Table 3.1 - Tracking NAS Changes and SRM Initiatives

Date	Description of Proposed Change	Accountable Office	SRM (Y/N) If No, provide justification	SRMD Developed by	Outcome/Result	Change Approved by

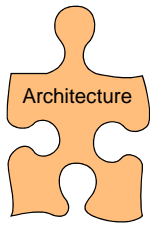
3.6 *How is the information in the tracking matrix used?*

The ATO Safety Service Unit reviews and analyzes the data, and when appropriate, provides feedback to the organizations concerning their use of SRM. This analysis also assists in identifying the scope of the SRM effort, as well as identifying the resource requirements to conduct SRM. The information will also be shared with AOV, which will assist them in identifying the scope of their oversight effort and provide insight into the processes used by the ATO to improve NAS safety.

3.7 *Where is SRM guidance available?*

Chapter 4, *Safety Risk Management Guidance*, contains more information regarding SRM, and Chapter 5, *Safety Risk Management Documentation: Development and Approval*, contains more information regarding the development of SRMDs.

The ATO Safety Service Unit can provide additional guidance concerning SRM and other SMS components, tools, and/or concepts.



Chapter 4 – Safety Risk Management Guidance

4.1 *What is the purpose of this guidance?*

This chapter is a systematic guide to the process of assessing and managing safety risk in the context of an SMS for the provision of air traffic services. These guidelines are in the form of:

- objectives for safety risk assessment and management processes
- descriptions of safety assessment activities early in planning or change proposal process to ensure safety management design considerations for achieving those objectives
- descriptions of the evidence and documentation that indicate that the objectives have been met

This guidance addresses changes to air traffic operations, maintenance, airspace and procedures development, airports, new systems, and modifications to existing systems (hardware and software).

Safety Risk Management (SRM) is conducted when proposed changes to the NAS (e.g., modifying existing or implementing new operations, procedures, and/or hardware and software systems) result in hazards that introduce risk, which must be mitigated. Ideally, SRM is performed early in the planning or change proposal process to ensure efficient real-time operations.

4.2 *What is Safety Risk Management?*

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

The SRM process ensures that safety-related changes are documented; risk is assessed and analyzed; unacceptable risk is mitigated; hazards are identified and tracked to resolution; the effectiveness of the risk mitigation strategies is assessed; and the performance of the change is monitored throughout its lifecycle.

4.3 *What is safety?*

Safety can be defined as freedom from unacceptable risk. Safety can be equated to some measurable goal. For example, an accident rate is less than an acceptable specified value.

4.4	<i>What is risk?</i>	Risk is the composite of predicted severity and likelihood of the potential effect of a hazard.
4.5	<i>What is a hazard?</i>	A hazard is any real or potential condition that can cause injury, illness, or death to people; damage to, or loss of, a system (hardware or software), equipment, or property; and/or damage to the environment. A hazard is a condition that is a prerequisite to an accident or incident.
4.6	<i>What is a system?</i>	A system is an integrated set of constituent pieces that are combined in an operational or support environment to accomplish a defined objective. These pieces include people, operational environment, usage, equipment, information, procedures, facilities, services, and other support services.
4.7	<i>What is an “error tolerant” system?</i>	Total elimination of risk is an unachievable goal. Even in organizations with the best training programs and a strong safety culture, human operators will occasionally make errors. The best-designed and maintained equipment will occasionally fail. It is important, therefore, that systems be 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. A system that meets these criteria is called an <i>error tolerant system</i> .
4.8	<i>How is an error tolerant system designed?</i>	<p>Developing a safe and error tolerant system requires a system to contain multiple defenses, barriers, and safeguards (including redundancy and design diversity) to ensure that, as much as possible, no single failure, error, or combination of failures and errors results in an accident. In a safe or error tolerant system, when a failure or error occurs, it is recognized, and corrective action is taken before a sequence of events leading to an accident can develop. Design attributes of error tolerant systems include:</p> <ul style="list-style-type: none">• make errors conspicuous (error evident systems)• trap the error to prevent it from affecting the system (error captive systems)• detect errors and provide warning and alerting systems (error alert systems)• ensure that there is a recovery path (error recovery systems) <p>There is a need for a series of defenses, rather than just a single defensive layer, because the defenses themselves may not always work as planned. This design philosophy is called <i>defenses-in-depth</i>.</p>

For an accident to occur in a system designed and implemented in accordance with these principles, gaps must occur in all the system's layers of defense at the critical time when that defense should have been capable of detecting the earlier failure or error. This is illustrated in Figure 4.1.

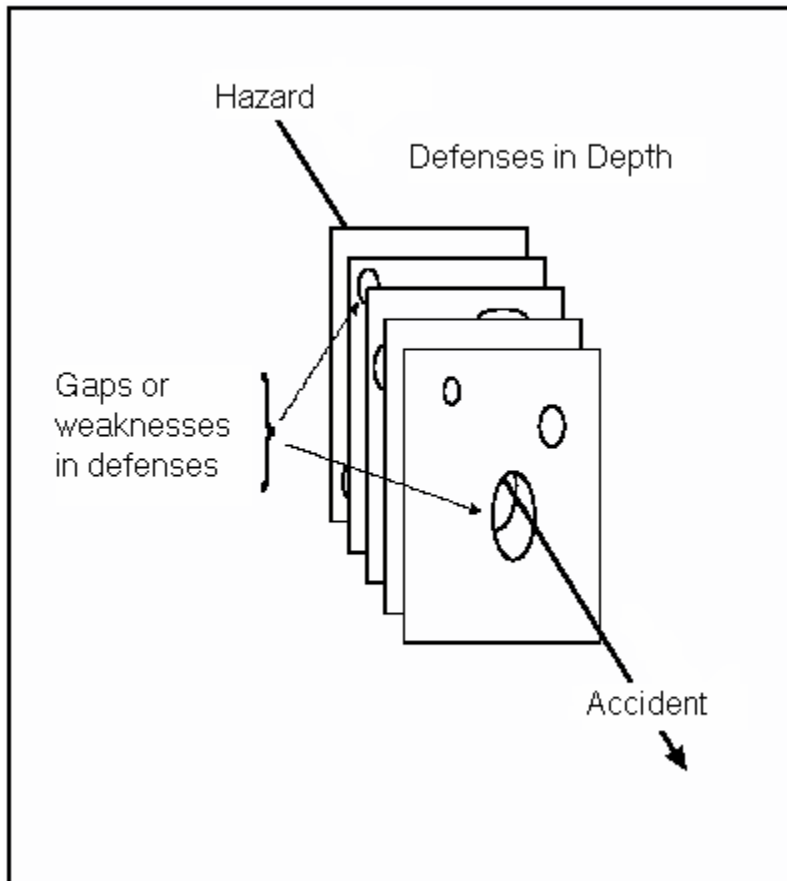


Figure 4.1 - Defenses in Depth Philosophy

The gaps in the system's defenses shown in Figure 4.1 are not necessarily static. Gaps “open” and “close” as the operational situation and environment changes, or equipment serviceability states change. A gap may sometimes be the result of nothing more than a momentary oversight on the part of a controller or operator. Other gaps may represent long-standing latent failures in the system.

4.9 *How are gaps detected?*

The principles outlined in this section may be applied to the task of reducing risk in both proactive and reactive ways. By careful analysis of a system combined with monitoring of operational data, it is possible to identify sequences of events where faults and

errors, either singly or in combination, could lead to an accident before an actual accident occurs. The same approach can also be used to analyze the chain of events that led to an actual accident after the fact. Identification of the active and latent failures revealed by this type of analysis enables corrective action to be taken to strengthen the system's defenses.

4.10 *How are gaps closed?*

The following defenses are typically used in combination to close gaps:

Equipment

- Redundancy:
 - p. full redundancy providing same level of functionality when operating on the alternate system
 - q. partial redundancy resulting in some reduction in functionality, e.g., local copy of essential data from a centralized network database
- Independent checking of design calculations and assumptions
- System designed to ensure a gradual degradation of capability (not total loss of capability) in the event of failure of individual elements
- Policy and procedures regarding maintenance, which may result in loss of some functionality in the active system, or loss of redundancy
- Automated aids, should always be subsidiary to safe and effective operating procedures that are the primary defense against the events, which these automated aids are designed to detect

Operating Procedures

- Read back of critical items in clearances and instructions
- Checklists and habitual actions, e.g., requiring a controller to follow-through the full flight path of an aircraft, looking for conflicts, immediate coordination is received from the handing-off sector
- Inclusion of a validity indicator in designators for standard instrument departures (SIDs) and standard terminal arrival routes

Organizational Factors

- Clear safety policy:
 - r. must be implemented with adequate funding provided for safety management activities
- Oversight to ensure correct procedures are followed:
 - s. no tolerance for violations or shortcuts
- Adequate control over the activities of contractors

For information regarding the preferred order for the development of risk mitigation controls, refer to Table 4.4 - *Safety Order of Precedence* in Section 4.52.

4.11 *How does change affect safety?*

Making changes to the NAS creates the potential for increased safety risk. SRM is used to improve the safety of the NAS by identifying, managing, and mitigating the safety risk of all safety significant changes (i.e., systems (hardware and software), equipment, procedures, etc.).

4.12 *How do hardware and software affect safety?*

Hardware components of the NAS are designed and fielded with specified and demonstrated levels of availability (availability is a function of reliability and maintainability). System redundancy and design diversity are used to provide service in the event of many, but not all, failures.

When a system includes software and/or firmware, the safety analyses consider possible design errors and the hazards they may create. Systematic design processes are an integral part of detection and elimination of design errors.⁷

4.13 *How does the human element affect safety?*

The performance of the human element within the air traffic services system cannot be specified as precisely as hardware. However, it is essential that the possibility of human error be considered as part of the overall design of the system. This requires analysis to identify potential weaknesses in the procedural aspects of the system. The analysis needs to take into account that accidents rarely have a single cause; they are usually the result of a combination of states or sequence of events. Therefore, the analysis needs to consider combinations of events and circumstances to identify sequences that could possibly compromise safety.⁸

4.14 *What is an SRM process?*

As depicted in Figure 4.2, a systematic SRM process proceeds through five general phases.

⁷ For additional guidance on the analysis of software and firmware, refer to the FAA System Safety Handbook (SSH) at <http://www.asy.faa.gov/Risk/SSHHandbook/cover.htm> and/or FAA software development standards (as describing in Radio Technical Commission for Aeronautics' (RTCA) DO-278 and DO-178). Both provide guidance on how to perform system safety engineering and management for FAA personnel involved in system safety activities

⁸ For more information regarding the role of human factors in evolving environments, refer to: FAA/NASA Human Factors for Evolving Environments: Human Factors Attributes and Technology Readiness Levels (at <http://www.hf.faa.gov/docs/508/docs/TRL.doc>).

These five phases are:

- describe the system
- identify the hazards
- analyze the risk
- assess the risk
- treat the risk (i.e., mitigate, monitor, and track)

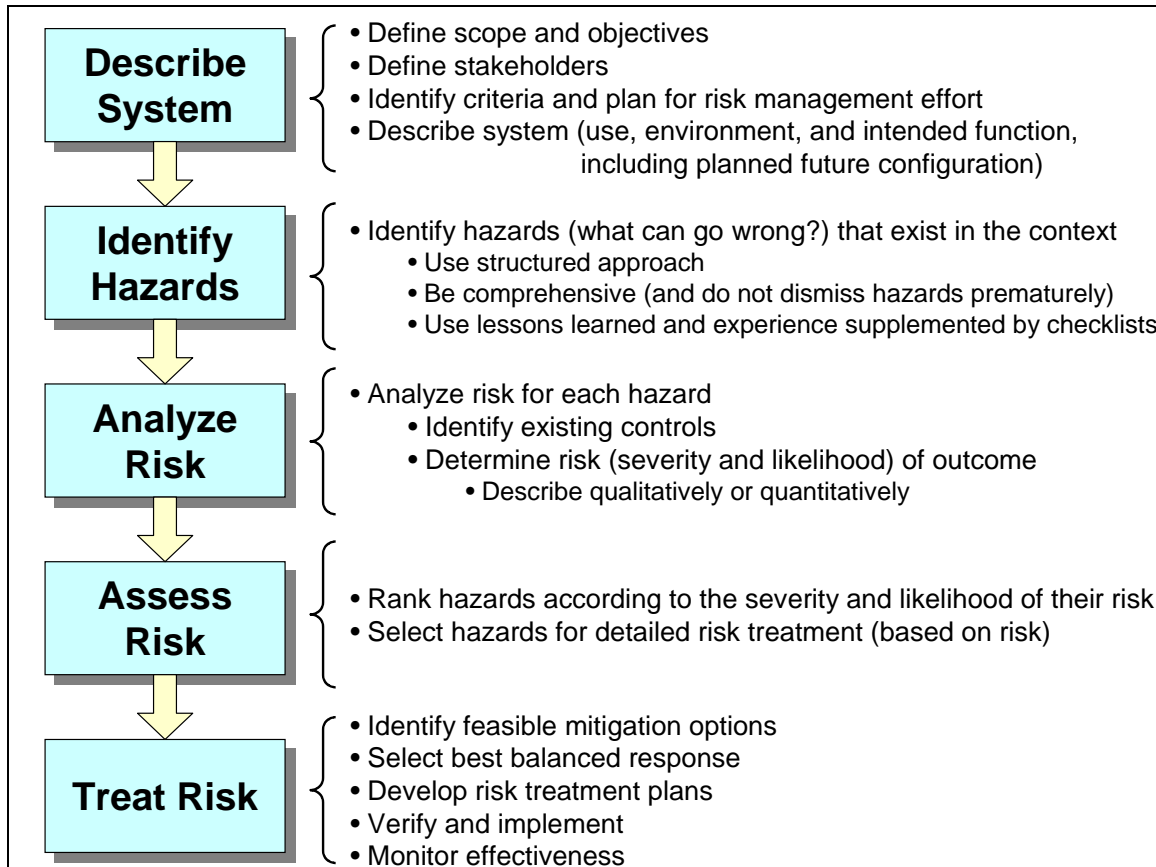


Figure 4.2 - Safety Risk Management Process

4.15 Phase 1: Describe the system

The “system” will always be a sub-component of some larger system. Even if the analysis encompasses all services provided within an entire Air Route Traffic Control Center, this can be thought of as a sub-set of a larger body of airspace, which in turn, is a subset of the NAS.

In describing the system:

- the scope of the problem or change is characterized and documented
- stakeholders are identified
- SRM is planned

- the system and operation are described and modeled in sufficient detail for the safety assessment to proceed to the next stage – identifying hazards

For more information on describing the system, refer to Section 4.26.

4.16 *Phase 2: Identify the hazards*

Once the system is described, hazards are identified. During this phase, things that can “go wrong” and the possible causes are identified and documented. The level of detail required in the hazard identification process depends on the complexity of the change being considered and the stage at which the assessment is being performed. A more comprehensive hazard identification process leads to more rigorous SRM. For more information on identifying the hazards, refer to Section 4.29.

4.17 *Phase 3: Analyze the risk*

In this phase, each hazard and the system state in which it potentially exists is evaluated to determine what exists to prevent or reduce the hazard’s effects or occurrence. The analysis compares a system and/or subsystem, performing its intended function in anticipated operational environments, to those events or conditions that would reduce system operability or service. These events may, if unmitigated, continue until total system degradation and/or failure occurs. These mitigations are called existing controls. Once the verified existing controls are determined and documented, an estimate of the hazard’s risk is made.

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

The hazard’s risk is the severity of the consequence and the likelihood of that consequence. The methods used to make this determination can be quantitative or qualitative depending on the application and the rigor used to analyze and characterize the risk. The analysis, both likelihood and severity, is heavily impacted by the failure modes of the system(s) under analysis. For more information on analyzing, refer to Section 4.38.

4.18 *Phase 4: Assess the risk*

In this phase, each hazard's risk is compared to and plotted on a pre-planned risk acceptability matrix. A hazard's priority is determined by its location on this risk matrix (Figure 4.9, Section 4.41). Higher priority hazards receive the greatest attention in the treatment of risk. For more information on assessing the risk, refer to Section 4.41.

4.19 *Phase 5: Treat the risk*

In this phase, options for dealing with risk are developed and managed. The risk management activity identifies feasible options to control or mitigate risk. While each will be discussed in detail later in this chapter, the options include:

- avoidance by selecting a different approach or not participating in the operation, procedure, or system development
- transfer to shift the risk to another area
- assumption to accept the likelihood and probability, and consequences associated with the risk
- research and knowledge to mitigate risk through expanding research and experience
- control to develop options and alternatives and/or take actions to minimize or eliminate the risk

The desired approach is selected and implemented. Prior to operational use, the mitigation strategy is validated and verified, and becomes an existing element of the system or operation. Table 4.4 - *Safety Order of Precedence* in Section 4.52 provides an overview of the preferred order for developing risk mitigation controls. For more information on treating the risk, refer to Section 4.43.

4.20 *The Bow-Tie (or Butterfly) model*

The approach to hazard analysis described in the previous sections can be illustrated using a Bow-Tie diagram. This diagram is useful in representing the link between causes, hazards, and effects. In this approach, it is assumed that each hazard can be represented by one or many causes that have the potential to lead to one or many effects (incidents or events).

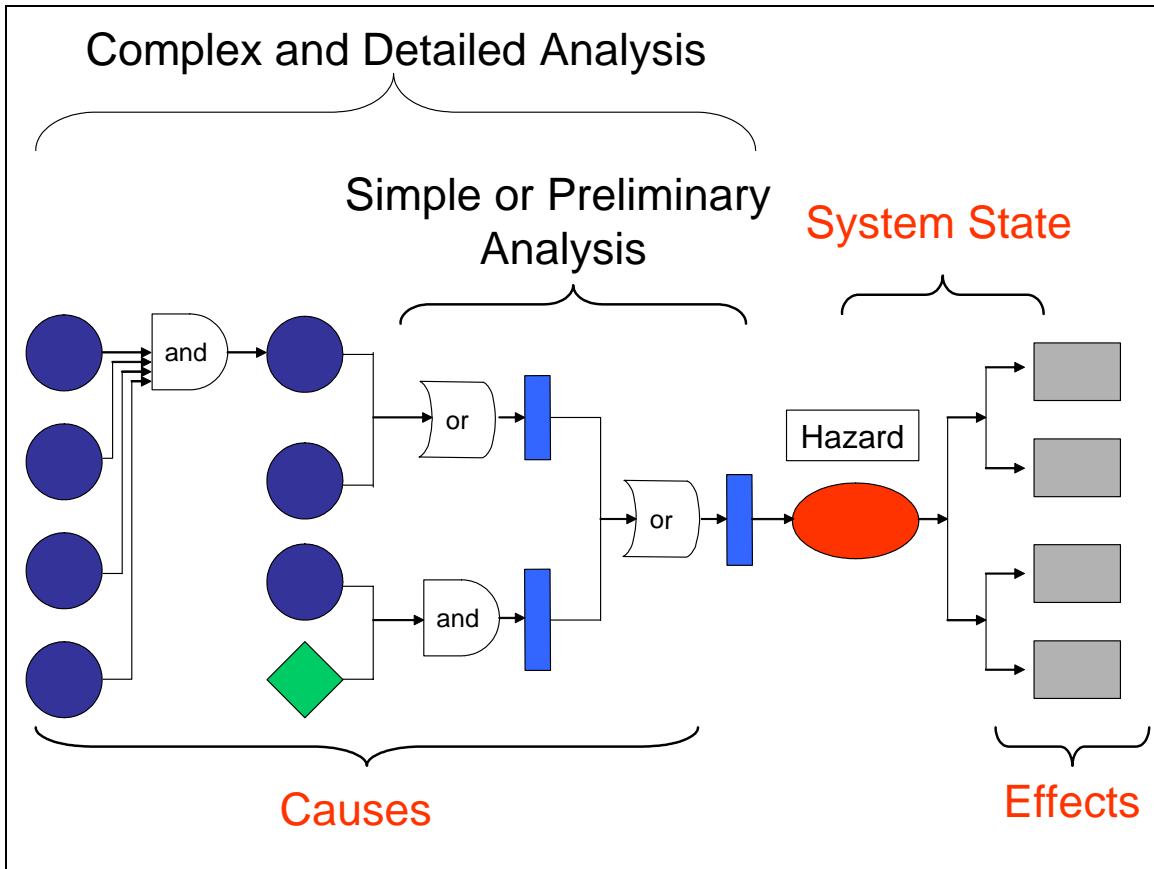


Figure 4.3 - The Bow-Tie Model

4.21 *The Bow-Tie model described*

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

The left hand side of the diagram can be viewed as a Fault Tree Analysis (FTA). The FTA is used to model the possible ways in which a given hazard could arise from causes in the system, taking into account mitigations that could be used to prevent failures that created the hazard.

The right side of the diagram can be viewed as an Event Sequence Analysis. The Event Sequence Analysis is used to model the system state and worst credible effect of a hazard, taking into account mitigations that could be incorporated to break an accident sequence in the event the hazard occurs.⁹

⁹ Note: certain causal chains can be extremely long if driven down to causal factors, such as cultural factors, which can become impractical to address.

Figure 4.4 illustrates the analysis of a hazard using the Bow-Tie model.

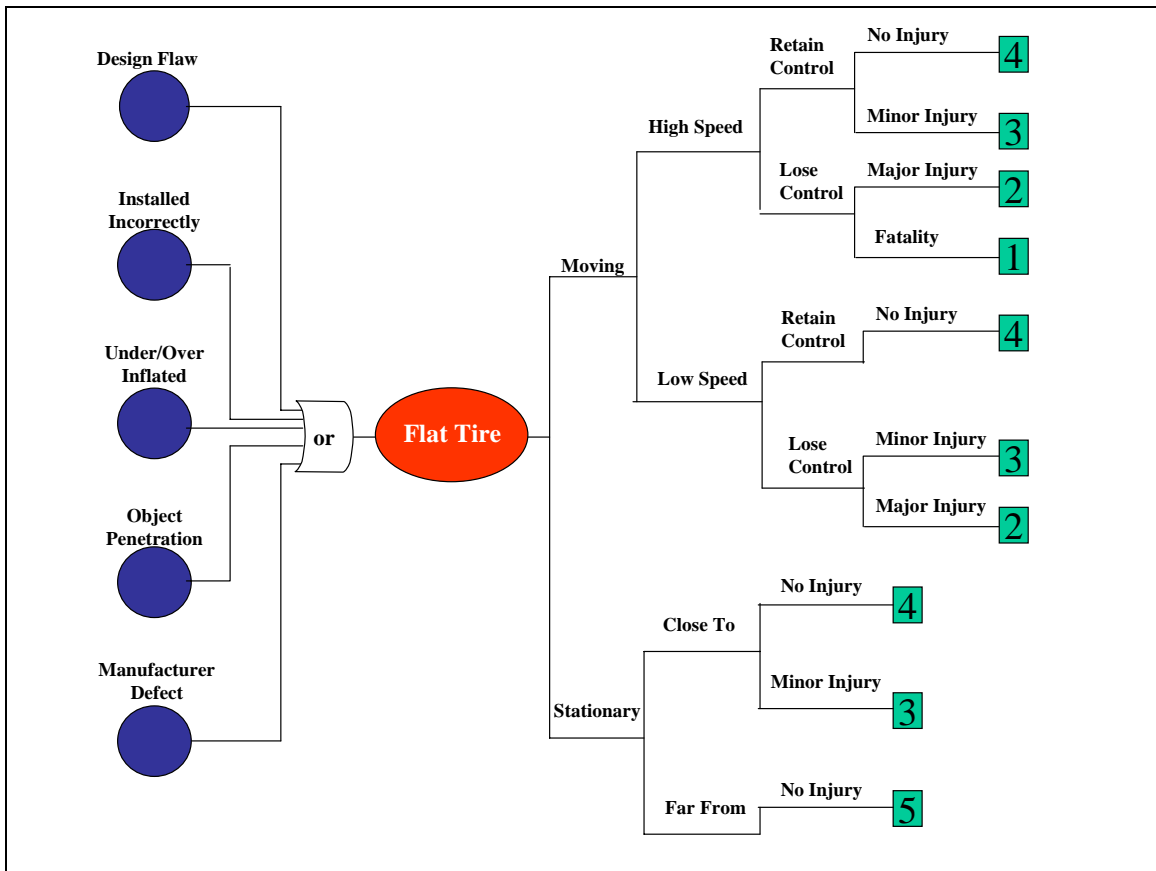


Figure 4.4 – Bow-Tie Model - Flat Tire Example

4.22 *Bow-Tie Model Example*

In Figure 4.4, the identified hazard is a flat tire. Some of the high-level causes are identified on the left side with circles. If this were an actual analysis, each cause would likely be broken down further into sub-causes. To the right of the hazard, the system state is identified as moving or not moving; and moving is further broken down into high and low speed and then into lose control and retain control. Each one of these system states results in an effect (injury and no injury). The effects have then been rated for severity (in the boxes), with one representing a catastrophic event and five representing no safety effect. The worst credible effect in this example occurs when a flat tire happens at high speed. Therefore, this is the sequence that would be used in the safety risk analysis.

4.23 *How deep and how wide should an analysis go?*

Selection of the appropriate scope and detail of the safety risk analysis is critical; multiple factors are taken into consideration. In general, SRM on more complex, expensive, and far-reaching changes will require increased scope and detail. For example, a \$1billion Acquisition Management System (AMS) program could require multiple safety assessments involving hundreds of pages of data at the preliminary, sub-system, and system levels looking at numerous interfaces with other systems in the NAS. On the other hand, an operational procedure change at a tower might be a smaller analysis resulting in a page or two describing the change and identifying the hazards and their risk. In both cases, the requirements of the SMS must be met, but the safety risk analysis is tailored to meet the needs of the decision-makers.

A primary consideration in determining both scope and detail of the safety risk analysis is: What information does the decision-maker need? In general, decision-makers need to know enough about the change, the associated hazards, and each hazard's risk to choose which controls to implement and when to accept the risk of the change.

Scope

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

- sufficient understanding of system boundaries to encompass possible impacts the system could have, including interfaces with peer systems and larger systems of which it is a component
- system elements
- limiting the system to those elements that affect or interact with each other to accomplish the mission or function

Depth

At a minimum, the safety risk assessment should detail the system and its hazards so that the projected audience can completely understand the safety risk. Guidelines to assist in determining detail include:

- more complex and/or increased quantity of functions will increase the number of hazards and hazard causes
 - complex and detailed analyses will delve deeply into multiple levels of hazard causes, sometimes in multiple safety risk analyses
 - hazards that are suspected to be high or medium risk should be thoroughly analyzed for causal factors and likelihood
-

4.24 How are the SRM phases accomplished?

The SRM process is consistent with ICAO guidelines and best practices. It is equally applicable to any safety risk management activity whether for operations, maintenance, procedures, or a new system development. Figure 4.5 describes the SRM process in more detail.

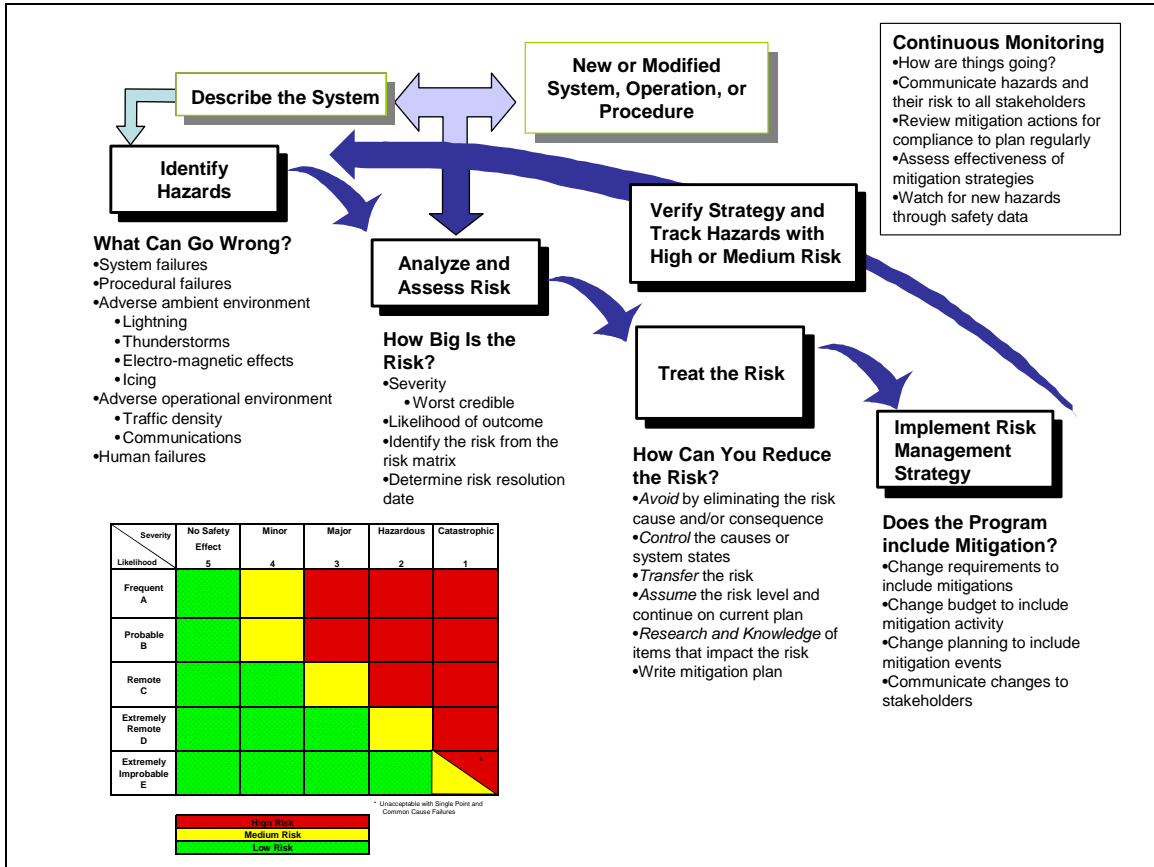


Figure 4.5 - Safety Risk Management Summary

4.25 What are the steps of SRM?

The phases of SRM can be broken down into twelve fundamental steps that, when completed, accomplish a thorough and consistent safety assessment.

The steps described in this section set a formal SRM effort apart from other safety systems. These steps apply to the entire scope of an organization’s operations, from system development, to operations and maintenance. These steps include:

Describe System

1. describe the system or operation that is being added or changed
2. plan the SRM effort

Identify Hazards

3. identify the hazards
4. identify hazard causes

Analyze Risk

5. assess the risk of the hazards
6. analyze existing controls

Assess Risk

7. rank hazards
8. prioritize hazards

Treat Risk

9. define risk management strategies
10. select risk management strategies
11. implement risk control strategies
12. verify control strategies (i.e., through monitoring and tracking)

The steps are closed-loop, meaning one or more steps are repeated until the safety risk for each hazard has been accepted. These steps are designed to ensure that those tasked with executing SRM are able to smoothly proceed through the SRM process.

The risk management effort continues until the residual risk is acceptable. Regardless of the phase of operation, these steps ensure that the FAA identifies and manages the safety risk associated with the provision of air traffic services.

These fundamental steps are depicted as a decision flow diagram in Figure 4.6.

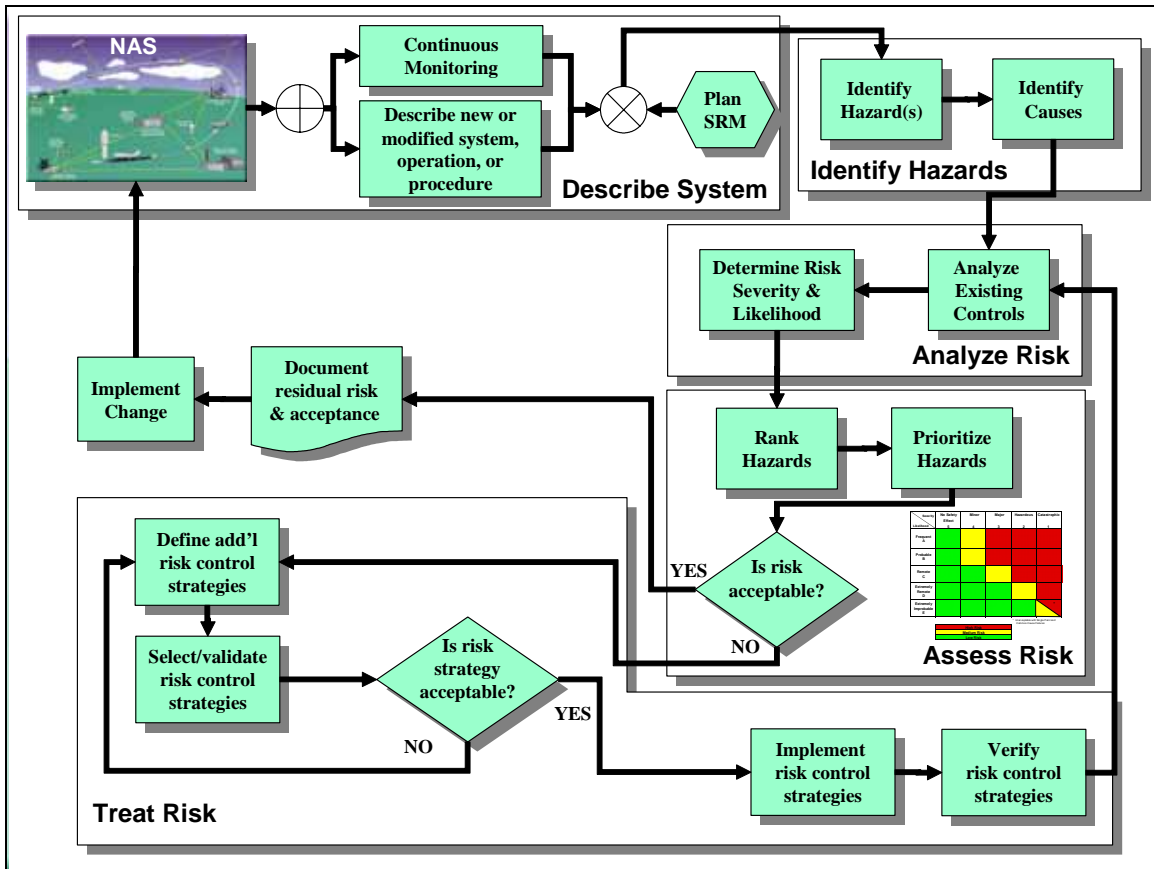


Figure 4.6 - Safety Risk Management Decision-Flow

Phase 1: Describe the System

4.26 *What are the elements of the system that can affect the system or interfacing systems?*

This phase of the process involves describing the system, (i.e., operation, equipment and/or procedures being added or changed), and planning the SRM effort. To ensure that all critical factors are taken into consideration, this stage is conducted carefully. The description that is produced in this step defines the scope of the risk assessment.

Whether a change involves new systems (hardware and software), operations, procedures, or a change to existing systems or procedures, a few fundamental steps apply to all. Whether it is a full report or a paragraph, any description of the change describes all the essential elements. Questions to consider include:

- What is the purpose of the system or change?
- How will the system or change be used?
- What are the system or change functions?
- What are the system or change boundaries and external interfaces?

- What is the environment in which the system or change will operate?

Figure 4.7 (5M Model) illustrates the elements of the NAS that should be considered in describing the system.

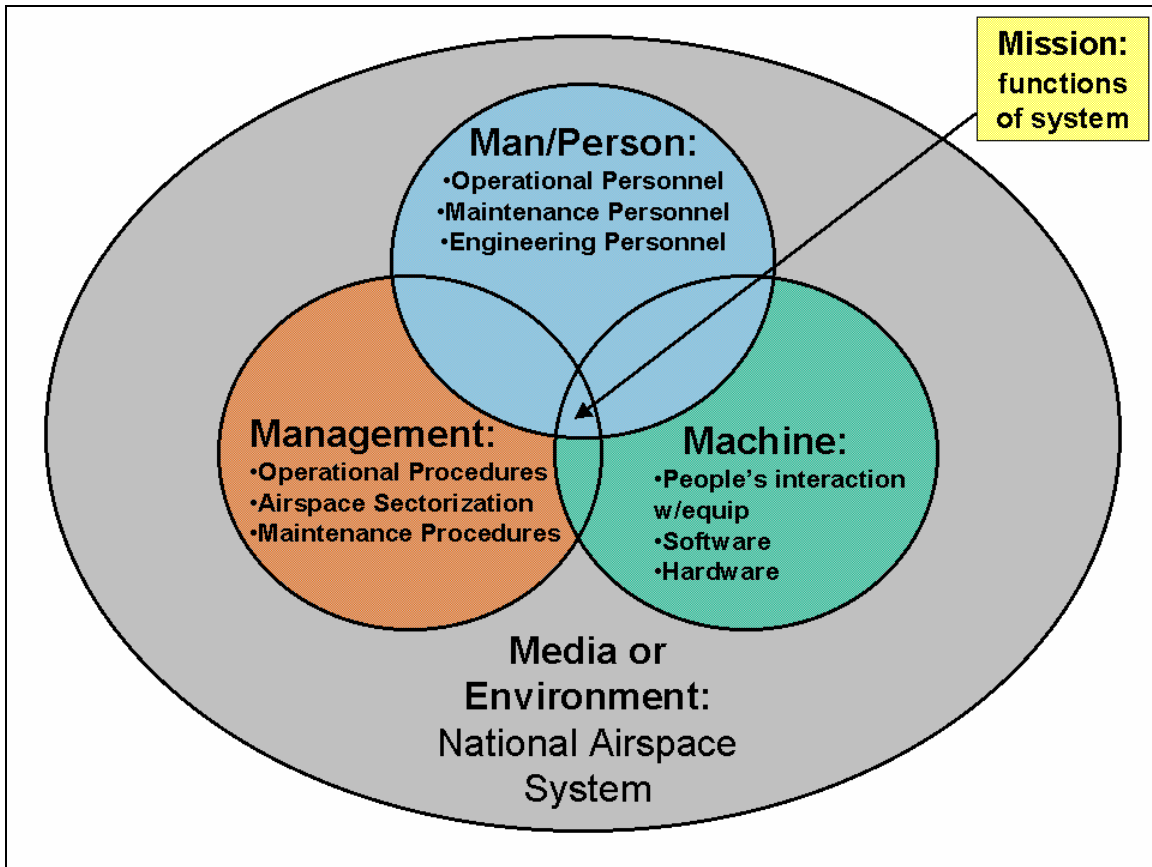


Figure 4.7 - 5M Model

4.27 *Is the system description correct and complete?*

System descriptions exhibit two essential characteristics: correctness and completeness. Correctness in a description means that it accurately reflects the system with an absence of ambiguity or error in its attributes. Completeness means that no attributes have been omitted and that the attributes stated are essential and appropriate to the level of detail. Descriptions that include all 5M Model elements demonstrate these two characteristics.

4.28 *What planning is needed for an SRM effort?*

Planning the safety risk assessment process requires:

- a determination of whether or not SRM is required

- a decision as to the level and type of safety risk assessment that is needed
- coordination with other organizations that may be affected by the change or the risk mitigation strategies

The effort can range from a single safety risk assessment to an entire SRM program. The determination of the scope of the SRM effort is a function of the nature, complexity, cost, and impact or consequence of the change. It is critical that the scope and complexity of the safety assessments match the scope and complexity of the change.

Phase 2: Identify Hazards

4.29 *What are the elements of hazard identification?*

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

- operational expertise
- training or experience in various hazard analysis techniques
- a defined hazard analysis tool

Managers ensure that operational expertise and safety experience and training are available to the safety assessment practitioner or team. Managers define data sources and measures to monitor for compliance with mitigation strategies. Data monitoring also helps detect more frequent or severe than expected hazards or less effective than expected mitigation strategies. Whoever performs the hazard analyses selects the tool that is most appropriate for the type of system being evaluated. Several hazard identification tools are listed in Table 4.1 (Section 4.37) with descriptions and references.

4.30 *What can go wrong?*

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

- the equipment (hardware and software)
- the operating environment (including physical conditions, airspace, and air route design)
- the human operators
- the human-machine interface (HMI)
- operational procedures
- maintenance procedures

- external services

4.31 What is a Hazard Model?

A hazard model is used to describe the relationship between system components, system and sub-system hazards, system states, and effects. Figure 4.8 provides a model of how the introduction of Reduced Vertical Separation Minima (RVSM) in an airspace system affects multiple organizations. It is important to note that, in addition to displaying ground components of the system, the diagram shows airborne components (on the aircraft), the safety of which will continue to be within the purview of AVR. However, the SMS will need to interface with AVR, as the airborne and ground components of the system continue to converge.

Hazard models highlight opportunities for cross-functional safety management and help ensure proper participation of organizations involved in hazard mitigation strategies.

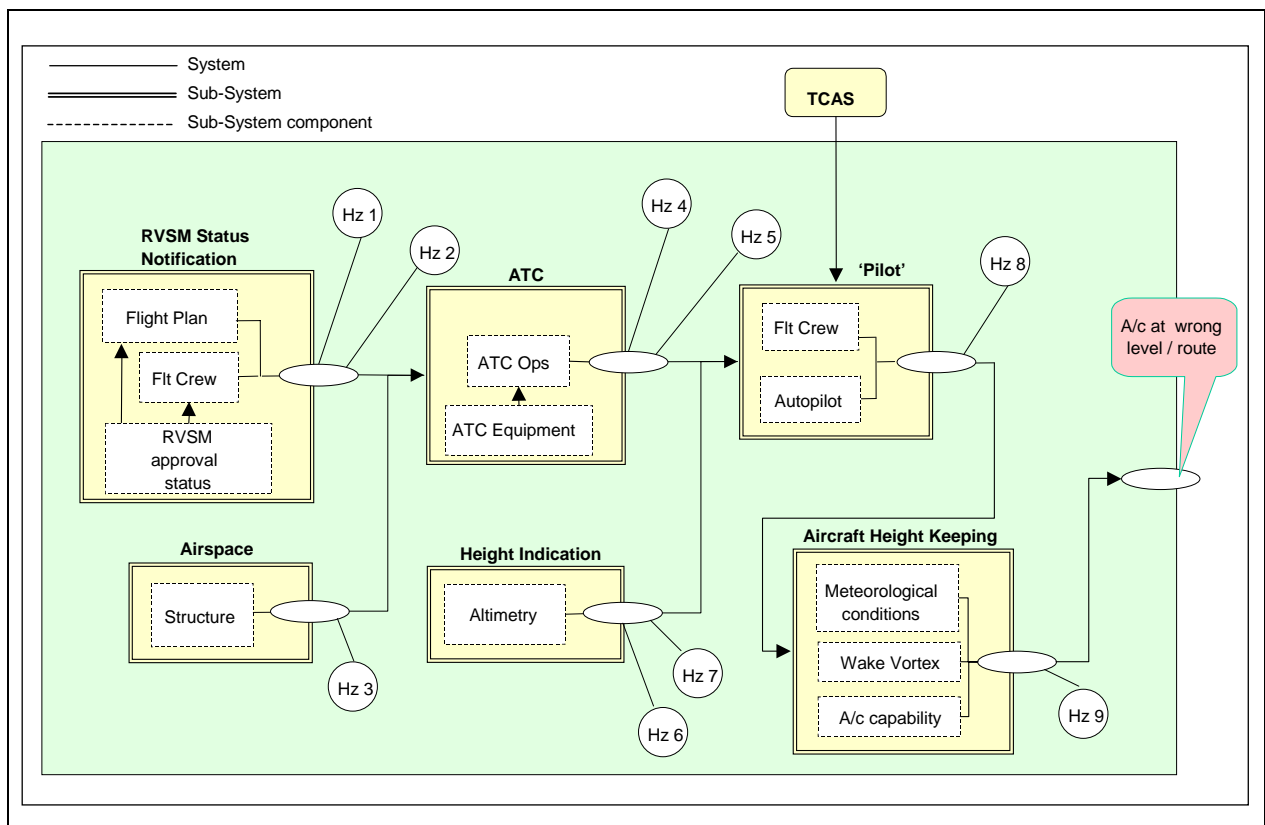


Figure 4.8 - System and Subsystem Hazards - Reduced Vertical Separation Minima (RVSM)¹⁰

¹⁰ EUROCONTROL, *Reduced Vertical Separation Minima (RVSM) Post-Implementation Safety Case (POSC)*, FHA Review Report, Issues 1.0, January 3, 2003 (modified and reproduced with permission).

4.32 *What is a hazard?*

A hazard is any real or potential condition that can cause injury, illness, or death to people, damage to, or loss of, a system (hardware and software), equipment, or property, and/or damage to the environment. A hazard is a condition that is a prerequisite to an accident or incident.

The FAA System Safety Handbook defines a hazard as "anything real or potential that could make possible or contribute to an accident. A condition that is a prerequisite to an accident." This definition is consistent with the Bow-Tie Model (Figure 4.3, Section 4.20) and the System and Subsystem Hazards (Figure 4.8).

The hazard is the adverse event that occurs as a result of the cause(s). In Figure 4.8, one overall hazard has been identified (i.e., *the aircraft is at the wrong level or route*). In addition, nine hazards were identified at the subsystem level.

4.33 *What are causes?*

Causes are events that lead to a hazard or hazardous condition. In Figure 4.8, Hazard 4 (Hz4) is the aircraft is at an inappropriate level. Hazard 4 could be caused by *the controller unintentionally assigning an aircraft to an inappropriate level*.

4.34 *What is system state?*

The system state refers to a variety of hazardous system conditions, including but not limited to:

- location
- system mode
- velocity
- operating rules in effect
- type of operation
- energy
- operational environment
- ambient environment

The system state is an expression of the various conditions, characterized by quantities or qualities in which the system can exist. System state can be described in:

- operational and procedural terms - Visual Flight Rules (VFR) vs. Instrument Flight Rules (IFR), Land and Hold Short Operations, etc.
- conditional terms - Instrument Meteorological Conditions (IMC) vs. Visual Meteorological Conditions (VMC), peak operating hours, etc.

- physical terms - Electromagnetic Environment Effects, precipitation, primary power source, back-up power source, etc.

In addition, for any given hazard, not all system states have equal risk.

The components of the system state are illustrated in Figure 4.8 (e.g., ATC operations and equipment, meteorological conditions, airspace structure, etc.).

4.35 Use the “worst credible” state.

To be consistent with the aim of ensuring safety, the assessment of hazards needs to make adequate allowance for worst-case conditions. However, it is also important that hazards included in the final analysis be *credible* hazards.

It is often difficult to draw the distinction between a worst credible case and one so dependent on coincidence that it need not be taken into account. The following definitions can be used as guides in making such decisions.

Worst – The most unfavorable conditions expected (e.g., extremely high levels of traffic, extreme weather disruption).

Credible – This implies that it is reasonable to expect the assumed combination of extreme conditions will occur within the operational lifetime of the change.

The assessment should always consider the most critical phase of flight within which an aircraft could be affected by the failure under consideration.

It is important to identify any potential *common mode failures*, which occur when a single event causes multiple failures of more than one function within a system.

4.36 What is the effect?

The effect (or harm) is a description of the potential outcome of the hazard if it occurs in the defined system state. In the RVSM example in Figure 4.8, the effects of aircraft being at the wrong level include:

- no safety effect
 - loss of separation, with no accident
 - mid-air collision
-

4.37 *What are Hazard Identification Tools?*

The following tools can be helpful in identifying hazards in operations, systems (hardware and software), or procedures. In many cases, the use of a single tool will suffice. However, some cases may require the use of more than one tool. Additional information about tools can be found in Appendix B.

Table 4.1 provides descriptions of a selection of hazard identification and hazard analysis tools. Appendix B provides more detailed information about the tools' utility and use. The source of the tools (except where otherwise noted) is the FAA's System Safety Handbook, which can be found at <http://www.asy.faa.gov/Risk/SSHandbook/cover.htm>.

Table 4.1 - Hazard Identification Tools

Tool or Method	Summary Description
Functional Hazard Analysis (FHA)	Uses Functional Analysis to determine "what" a system (e.g., equipment procedures or operations) must do in order to complete a mission or higher function. The failure or anomalous behavior of these functions is identified as a hazard and ranked according to severity based on its operational effect.
Fault/Failure Hazard Analysis	Tool to identify and evaluate component hazard modes, determine causes of these hazards, and determine resultant effects to the subsystem and its operation.
Failure Modes and Effects Analysis (FMEA) and Failure Modes, Effects, and Criticality Analysis (FMECA)	Hypothesizes failure events, which impact the operation or system. These events are identified as hazards. Often used as an input to a sub-system hazard analysis.
Operations Analysis	This provides an itemized sequence of events or flow diagrams depicting the major events of an operation or system. Failure or anomalous behavior in these events is identified as a hazard.
Preliminary Hazard Analysis (PHA)	The PHA provides an initial overview of the hazards present in the overall flow of the operation. It provides a hazard assessment that is broad, but usually not deep.
"What if..." Tool	The "what if..." tool is a brainstorming method. It is designed to add discipline and structure to the experiential and intuitive expertise of operational personnel.
Scenario Process Tool	Hazards are identified by visualizing events or sequences of events where things go wrong. Like the "what if ..." tool, it is designed to capture the experiential and intuitive expertise of operational personnel.
Logic Diagram	Diagrams events in their logical relationships. These events or their anomalous behavior are identified as hazards.
Change Analysis	Identifies planned and potential unplanned changes to a system (e.g., operation, equipment, or procedure). Hazards are then identified, using one of the other tools.

Tool or Method	Summary Description
Cause and Effect Tool	Also known as the “fish bone” and Ishikawa Diagram. This is a variation of the Logic Diagram. Effects are depicted as horizontal lines with causes entering the effect line diagonally (like a fish bone). The result is the hazard.
Hazard and Operability Tool (HAZOP)	Highly structured hazard identification tool. It uses a standard set of guide terms that are then linked to a tailored set of process terms. Each link is evaluated for its validity. Valid links are identified as hazards.
Mapping Tool	Also known as Map Analysis and Zonal Safety Analysis. Uses models and schematics to identify and evaluate hazards and hazard causes. Depicts energies and sources of hazards relative to vulnerable entities.
Interface Analysis	Used to discover the hazardous linkages between interfacing systems.
Accident and Incident Analysis	Uses data on recorded hazardous events. These events are grouped in various ways according to a pre-established criteria usually a common cause or outcome. The groupings are identified as hazards.
Interview Tool	Knowledgeable operational personnel are queried or interviewed confidentially. They are asked to freely describe things that have gone or could go wrong in a system.
Inspection Tool	Also called the Survey Tool. Hazards are identified by direct observation of a system.
Job Hazard Analysis (JHA)	Used to examine the safety of a single job in detail. The job is broken down into individual stages. Each stage is then analyzed for events associated with that stage that can go wrong. These events are identified as hazards.
Opportunity Assessment	Identifies opportunities for expansion of an organization’s capabilities. Risk-related barriers to this expansion are identified as hazards. The hazards are then risk managed.
Energy Trace-Barrier Analysis (ETBA)	Highly structured. Documents all energy sources in system. The energy sources are identified as hazards. Barrier between the energy sources and the operators, maintainers, and other systems are identified as mitigations.
Fault Tree Analysis (FTA)	Similar to a negative Logic Diagram but with the addition of symbols (and, or, and/or, exclusion) that aid in the assessment of probability.
Multi-Linear Event Sequencing Tool (MES)	Also called the timeline tool and the sequential time event plot (STEP). ¹¹ Used to detect hazards from the time relationship between various operational or systemic events.
Management Oversight and Risk Tree (MORT)	Very structured and time-consuming. Very detailed logic diagram useful for assessing the highest risks and most operational critical activities.
FAA Operational Support Test and Evaluation (T&E) Gold Standard for National Airspace Systems Hardware and Software Modifications	Multi-step process used by all FAA secondary maintenance organizations to design, develop, test and evaluate, and deliver hardware and software modifications to existing operational NAS systems. This process ensures that existing functionality is maintained and that modifications add new capability or improve existing capability. All safety significant functionality is verified with each delivered product baseline.

¹¹ K. Hendrisk, and L. Benner. *Investigating accidents with STEP*. Marcel Dekker, New York, 1988.

Phase 3: Analyze Risks

4.38 *What are the existing controls?*

In this phase, each hazard and the system context in which it potentially exists are evaluated to determine what exists to prevent or reduce the hazard's occurrence or mitigate its effects. These mitigations are called existing controls. An existing control can only be a control that has been validated or verified.

4.39 *What is severity, and how is it related to risk assessment?*

Risk is the composite of the predicted severity and likelihood of the outcome or effect (harm) of the hazard in the worst credible system state. In order to assess the risk of a hazard occurring, severity and likelihood are first determined.

Severity is determined by the worst credible potential outcome. Less severe effects may be considered analytically in addition to this, but at a minimum, the most severe effects are considered. Do not consider likelihood when determining severity. Determination of severity is independent of likelihood.

Table 4.2 provides specific severity definitions for use in this phase.

Table 4.2 - Severity Definitions

Effect On: ↓	Hazard Severity Classification				
	No Safety Effect	Minor	Major	Hazardous	Catastrophic
General		Does not significantly reduce system safety. Required actions are within operator's capabilities. Includes (see below):	Reduces the capability of the system or operators to cope with adverse operating conditions to the extent that there would be a (see below):	Reduces the capability of the system or the operator's ability to cope with adverse conditions to the extent that there would be a (see below):	Total loss of systems control such that (see below):
Air Traffic Control	Slight increase in ATC workload	Slight reduction in ATC capability, or significant increase in ATC workload	Reduction in separation as defined by a low/moderate severity operational error (as defined in FAA Order 7210.56), or significant reduction in ATC capability	Reduction in separation as defined by a high severity operational error (as defined in FAA Order 7210.56), or a total loss of ATC (ATC Zero)	Collision with other aircraft, obstacles, or terrain
Flying Public¹²	<ul style="list-style-type: none"> - No effect on flight crew - Has no effect on safety - Inconvenience 	<ul style="list-style-type: none"> - Slight increase in workload - Slight reduction in safety margin or functional capabilities - Minor illness or damage - Some physical discomfort 	<ul style="list-style-type: none"> - Significant increase in flight crew workload - Significant reduction in safety margin or functional capability - Major illness, injury, or damage - Physical distress 	<ul style="list-style-type: none"> - Large reduction in safety margin or functional capability - Serious or fatal injury to small number - Physical distress/excessive workload 	Outcome would result in: <ul style="list-style-type: none"> - Hull loss - Multiple fatalities

¹² For more information regarding these definitions, refer to FAA Advisory Circular 25.1309-1A, *System Design Analysis*, 06-21-88.

4.40 *What is likelihood, and how is it related to risk assessment?*

Remember that risk is the composite of the predicted severity and likelihood of the outcome or effect (harm) of the hazard in the worst credible system state. Likelihood is an expression of how often an event is expected to occur.

Severity must be considered in the determination of likelihood. Likelihood is determined by how often the resulting harm can be expected to occur at the worst credible severity. When determining likelihood, the worst credible system states will usually determine the worst credible severity.

Likelihood definitions should be tailored to the domain and service. Table 4.3 provides likelihood definitions that could be used in this step or could be used as information to support developing definitions that work for the change to be assessed.

NAS Systems' likelihood definitions (first three columns) are currently in use when acquiring new systems. Flight Procedures definitions (the fourth column) are used by Flight Standards (AFS) in assessing flight procedures. ATC Operational definitions (the last two columns) are proposed likelihood definitions for use in assessing ATC operations (e.g., airspace changes, ATC procedures and standards, etc.).

Appendix C contains information and guidance on applying SRM to ATC procedural changes.

Table 4.3 - Likelihood Definitions

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

Phase 4: Assess the Risk

4.41 What is a risk matrix?

An estimation of risk is determined using the predictive risk matrix in Figure 4.9.

The risk levels used in the matrix can be defined as:

- **High risk** – Unacceptable risk - proposal cannot be implemented unless hazards are further mitigated so that risk is reduced to medium or low level and AOV approves the mitigating controls. Tracking and management are required. Catastrophic hazards that are caused by: (1) single-point events or failures, (2) common cause events or failures, or (3) undetectable latent events in combination with single point or common cause events are considered high risk, even if extremely remote. (Note: high risk is unacceptable at the time of hazard closure. However, for short periods of time, high risk may exist while mitigation plans are put into affect.)
- **Medium risk** – Acceptable risk - minimum acceptable safety objective; proposal may be implemented, but tracking and management are required.
- **Low risk** – Target - acceptable without restriction or limitation; hazards are not required to be actively managed but are documented.

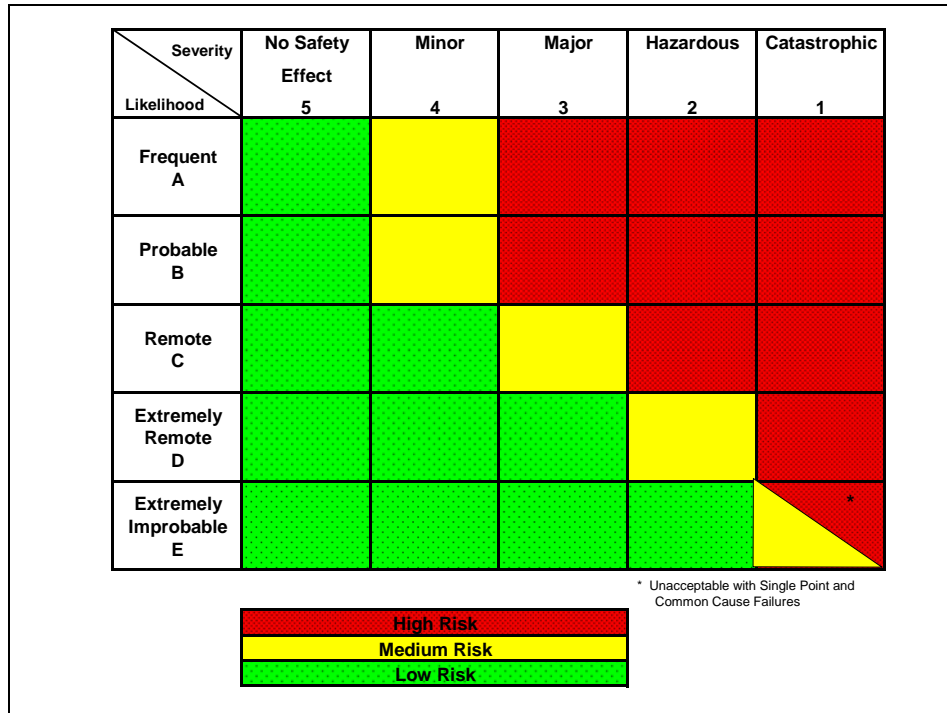


Figure 4.9 - Predictive Risk Matrix

4.42 *How are risks ranked and prioritized?*

Hazards are ranked according to the severity and the likelihood of their risk, which is illustrated by where they fall on the risk matrix. Hazards with high risk receive higher priority for treatment and mitigation.

Phase 5: Treat Risk

4.43 *Why define risk management strategy?*

In this phase, alternative strategies for managing a hazard's risk are developed. These strategies become actions that reduce the risk of the hazard's effects on the system (e.g., operation, equipment, or procedure). It should be noted that the majority of risk management strategies address medium and high risk hazards. Low risk hazards are, by definition, adequately controlled.

4.44 *What is risk mitigation?*

Risk mitigation can be:

- revision of the system design
- modification of operational procedures
- establishment of contingency arrangements

The effect of the proposed mitigation measures on the overall risk is assessed. If necessary, the process is repeated until a combination of measures is found that reduces the risk to an acceptable level.

When risk is determined to be unacceptable, it is necessary to identify and evaluate risk mitigation measures by which the probability of occurrence and/or the severity of the hazard could be reduced. When risk mitigation strategies cross organizations, risk acceptance and approval from those stakeholder organizations is necessary, in accordance with Table 4.5 in Section 4.61 and Table 5.1 in Section 5.6.

In cases where systemic hazards are identified, impacted managers must identify and implement risk mitigation efforts.

4.45 *What are some risk mitigation actions?*

Risk mitigation requires a conscious management decision to approve, fund, schedule, and implement one or more risk mitigation strategies. The objective of this phase is to implement appropriate and cost-effective risk mitigation plans to mitigate hazards. Appropriate risk mitigation strategies are developed, documented, selected, and implemented. Hazard tracking is the core of this risk management phase.

Risk mitigation actions are separated into one, or a combination, of the following categories:

- avoidance
- transfer
- assumption
- research and knowledge
- control

Once risk mitigation strategies are selected and developed, the impact on other organization(s) is also identified, and those strategies are coordinated with, and agreed to by, the affected organizations(s).

4.46 *What is an avoidance strategy?*

Avoidance is a strategy to avert the potential of occurrence and/or consequence by selecting a different approach or by not participating in the operation, procedure, or system (hardware and software) development. This technique may be pursued when multiple alternatives or options are available. It is more likely used as the basis for a "Go" or "No-Go" decision at the start of an operation or program. The avoidance of risk is from the perspective of the overall organization. Thus, an avoidance strategy is one that involves all the stakeholders to the proposed change. This strategy permits an organization-wide avoidance of the risk.

4.47 *What is a transfer strategy?*

Transfer is a strategy to shift the risk to another area such as another operation, requirement, organization, supplier, or a stakeholder. Examples include reallocation of operations, requirements, securing supplier product warranties, and negotiation of fixed-price contracts with vendors. Note that at the operational or organizational level, the risk remains. The transfer of the risk is accomplished primarily to optimize the overall operational risk and to assign ownership to the organization or operation most capable of reducing the risk. It is possible that the risk level will change as a result of the risk transfer.

Transference, while an acceptable means of dealing with risk, cannot be the only method of mitigation used to treat a high risk hazard. The risk must still be mitigated to medium or low before it can be accepted in the NAS.

4.48 *What is an assumption strategy?*

Assumption is simply accepting the likelihood or probability and the consequences associated with a risk's occurrence. Assumption is usually limited to low risks.

An assumption strategy cannot be the only method of mitigation used to treat a high risk hazard. The risk must still be mitigated to medium or low before it can be accepted into the NAS.

4.49 *How can research and knowledge mitigate risk?*

Research and knowledge may mitigate risk through expanding experience. Since some risk arises from uncertainty and inexperience, it may be possible to effectively mitigate risk simply by enlarging the knowledge pool. This could lead to a reassessment that reduces the likelihood of failure or provides insight into how to lessen the consequences.

4.50 *What is a control strategy?*

Control is a strategy of developing options and alternatives, and taking actions that lower or eliminate the risk. Examples include new concepts, more analysis, redundant systems and/or components, and alternate sources of production. A control is anything that reduces a hazard's risk.

A hazard control is always written in requirements language. When this is done, the "control" becomes a "safety requirement." Controls can be complex or simple. The important aspect is that they are effective and verified before the change is approved for operation.

4.51 *What is the status of a control?*

Controls can be in three states of existence:

- Validated - Validated controls are those controls and requirements that are unambiguous, correct, complete, and verifiable
- Recommended - Recommended controls are those controls that have the potential to mitigate a hazard or risk but have not yet been validated as part of the system or its requirements
- Verified - Verified controls are those controls and requirements that have met the implemented solution

4.52 *What is the preferred order of controls?*

There is a preferred order for the development of risk mitigation controls. This order is reflected in the safety order of precedence shown in Table 4.4.

Table 4.4 - Safety Order of Precedence

Description	Priority	Definition	Example
Design for minimum risk	1	Design the system (e.g., operation, procedure, or equipment) to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level through selection of alternatives.	<ol style="list-style-type: none"> 1. If a collision hazard exists because of a transition to a higher Minimum En route Altitude at a crossing point, moving the crossing point to another location would eliminate the risk 2. If “loss of power” is a hazard to a system, adding a second independent power source reduces the likelihood of the “loss of power” hazard
Incorporate safety devices	2	If identified risks cannot be eliminated through alternative selection, reduce the risk via the use of fixed, automatic, or other safety features or devices, and make provisions for periodic functional checks of safety devices.	<ol style="list-style-type: none"> 1. An automatic “low altitude” detector in a surveillance system 2. Ground circuit in refueling nozzle 3. Automatic engine restart logic
Provide warning	3	When neither alternatives nor safety devices can effectively eliminate or adequately reduce risk, warning devices or procedures are used to detect the condition and to produce an adequate warning. The warning must be provided in time to avert the hazard effects. Warnings and their application are designed to minimize the likelihood of inappropriate human reaction and response.	<ol style="list-style-type: none"> 2. A warning in an operators manual 3. “Engine Failure” light in a helicopter 4. Flashing warning on a radar screen
Develop procedures and training	4	Where it is impractical to eliminate risks through alternative selection, safety features, and warning devices: procedures and training are used. However, concurrence of management authority is required when procedures and training are solely applied to reduce risks of catastrophic or hazardous severity.	<ol style="list-style-type: none"> 1. A missed approach procedure 2. Training in stall/spin recovery 3. Procedure to vector an aircraft above a Minimum Safe Altitude on a VHF Omni-directional Range (VOR) airway 4. Procedures for loss of communications

4.53 *What if the risk cannot be sufficiently reduced?*

If the risk cannot be reduced to an acceptable level after all possible mitigation measures have been attempted, the change does not satisfy the safety requirements; therefore, it is necessary to either revise the original objectives or abandon the proposal.

4.54 *What is hazard tracking?*

Each medium and high risk hazard is tracked until its risk is mitigated to low, as defined in Section 4.41, and the effectiveness of the controls mitigating the risk are verified. The hazard record is kept for the lifecycle of the change.

Hazard tracking and risk resolution (HTRR) is a closed-loop method of ensuring that the requirements and mitigations associated with each medium and high risk hazard are implemented. In addition, HTRR ensures that before a hazard is

accepted, it is evaluated for residual risk. HTRR is an inherent part of analyzing risk, assessing risk, and treating risk.

In an operating environment with limited available resources, the Agency necessarily focuses its attention and resources on the most important hazards. The best measure of a hazard's importance is its risk. Therefore, the highest risk hazards are treated with the greatest care and receive the most mitigation effort; HTRR follows this principle.

Low risk hazards by definition meet the FAA's safety requirements for risk level and require no further mitigation. High risk hazards, on the other hand, require tracking and must be further mitigated before they are acceptable. There is some uncertainty in any risk assessment, so medium risk hazards are included in HTRR as well.

HTRR is the process of defining additional safety requirements, verifying implementation, and re-assessing the risk to make sure the hazard meets its risk level requirement before being accepted. Tracking implies that a system is used to document the hazard's life cycle, as well as decisions made. This system can be a database, spreadsheet, or something as simple as a notebook. The FAA has a restricted access, web-based Hazard Tracking System (HTS) that meets the requirement for HTRR.

4.55 *What else should be considered in SRM?*

If a system change is very large or complex, the manager responsible for the SRM should consider convening a panel of subject matter experts to assist in hazard identification.

4.56 *What is an SRM Panel?*

A single practitioner may complete a change that is not complex. However, complex system changes may require that a panel of subject matter experts be convened to identify hazards, establish mitigations, and assess risk. If a panel of experts is to be convened, it needs to include representatives of the various organizations concerned with the specification, development, and use of the system.

4.57 *How should an SRM panel be conducted?*

The interactions between participants with varying experience and knowledge tend to lead to broader, more comprehensive, and more balanced consideration of safety issues than if an individual conducts the assessment.

While group sessions are usually good at generating ideas, identifying issues, and making an initial assessment, they do not

always produce these outputs in a logical order. In addition, it is difficult for a group to analyze the ideas and issues in detail, since it is hard to consider all the implications and inter-relationships between issues when they have only just been raised. Much time can be wasted in highly technical discussions that may turn out to be irrelevant.

Therefore, it is recommended that:

1. The group session is used to generate ideas and undertake preliminary assessment only (perhaps identifying factors which are important, rather than working through the implications in detail).
2. The findings are collated and analyzed after the session. This is normally done by one or two individuals with sufficient breadth of expertise to understand all the issues raised and a good appreciation of the purposes of the assessment. The person who facilitated or recorded the session often is best able to perform this task.
3. The collated results are presented to the group to check that input has been correctly interpreted and to provide an opportunity to reconsider any aspect once the whole picture can be seen.

4.58 *How does SRM affect safety levels?*

Utilization of safety risk management increases the level of safety in air traffic services operations, maintenance, airspace and procedures development, and new systems. Through SRM, hazards are assessed, mitigated, documented, tracked, and operational data are continuously monitored to provide feedback on hazards. Understanding the consequences of risk increases the ability to anticipate and control the impacts of internal and/or external events on a program.

Through SRM, an essential function of the SMS, decision-makers are better able to manage and reduce risk leading to increased safety.

4.59 *What does it mean to accept the safety risk of a change?*

Accepting the safety risk is a certification by the appropriate management official that he/she understands the safety risk associated with the change and he/she accepts that safety risk into the NAS. This is different from approving the documentation of safety risk management, in which the approving party agrees that the analysis accurately reflects the safety risk associated with the change, the underlying assumptions are correct, and the findings are complete and accurate.

4.60 *Who can accept the safety risk?*

The acceptance of the safety risk is dependent on the span of the program, its associated risk, and the mitigation used to control the risk. Only those who own the change and are in a position to manage the risk can accept the risk into NAS.

Changes that have high initial safety risk, where safety risk and/or controls/mitigations:

- stay within ATO Service Unit; the safety risk is accepted by the Service Unit VP
- span ATO Service Units; the safety risk is accepted by each affected Service Unit's VP
- go outside of the ATO (i.e., to ARP and/or AVR); the safety risk is accepted by the ATO Service Unit VP and the heads of each affected LOB

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

- stay within ATO Service Unit; the safety risk is accepted by the appropriate management official within the Service Unit
- span ATO Service Units; the safety risk is accepted by the appropriate management officials within each affected Service Unit
- go outside of the ATO (i.e., to ARP and/or AVR); the safety risk is accepted by the appropriate management officials within each affected ATO Service Unit and LOB

Risk acceptance requirements are summarized in Table 4.5.

Table 4.5 - Risk Acceptance Summary

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

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

4.61 *What is the ATO Safety Service Unit and/or AOV's role in accepting safety risk?*

Neither the ATO Safety Service Unit nor AOV has a role in accepting safety risk. Only operational owners of NAS components can accept risk because only they can manage risk by employing controls. However, LOBs outside of the ATO (ARP and AFS) do have a role in accepting safety risk because they own components of the NAS. Therefore, ATO managers, directors, and VPs must work closely with their counterparts in these LOBs to ensure that the appropriate party or parties are accepting and managing safety risk resulting from NAS changes.

4.62 *In addition to SRM, what else is done before a change is implemented in the NAS?*

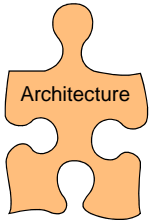
In addition to SRM, the FAA verifies that a new or modified system (hardware and software) is ready to be used in the operational environment for which it is intended. The method of verification depends on the nature of the change and is tailored to the need. However, verification must show that the requirements have been met and the system performs its intended function(s).

Methods of verification include: test, analysis, examination, and demonstration/evaluation. For more information, see the FAA System Engineering Manual (SEM) and/or the T&E Gold Standard process in Appendix B.

4.62 *Where can I get more information regarding SRM or receive help in conducting SRM?*

Each ATO Service Unit has a designated Safety Manager who can provide additional guidance regarding the SMS and/or SRM. In addition, each service unit will also have Senior Safety Engineers (SSEs) who will provide SRM expertise. Both, the Safety Manager and/or SSE will be available to provide input to the management official(s) who will accept the risk associated with the change. In addition, if risk must be accepted outside the service unit, the Safety Manager and/or SSE will help to facilitate that coordination.

As with any other SMS component or topic in this manual, the ATO Safety Service Unit is also available to provide additional guidance and/or information.



Chapter 5 – Safety Risk Management Documentation: Development and Approval

5.1 *What SRM documentation is required?*

The proper documentation of safety risk assessments is an important part of conducting the assessment. Both the results of the assessments and the decisions made when determining if safety assessments are required (Section 3.1) are documented and kept on file for the life of the proposed change.

5.2 *What is an SRMD?*

A Safety Risk Management Document (SRMD) is a report that thoroughly describes the SRM process for a given proposed change and documents the evidence to support that the proposed change to the system is acceptably safe. That is to say, that the risk associated with the proposed change is acceptable.

5.3 *What is in an SRMD?*

An SRMD contains, at a minimum:

- description of the potential system state(s) – including identification of any important support systems and interfaces without which the system could not achieve its functional intent
- description of the proposed change
- identified hazards (and description of hazard identification methodology)
- estimation of risk
- description of existing and planned mitigation
- description of methodology for tracking hazards and verifying effectiveness of mitigation controls throughout the lifecycle of the system or change
- method for monitoring operational data to ensure hazards are controlled
- identification of the organization responsible for the conduct of the analysis and tracking of the resolution, if any
- current disposition of hazard mitigations
- plan to verify that safety critical performance requirements are met
- a recommendation concerning the implementation decision

(Note: An in-depth description of SRM can be found in Chapter 4, *Safety Risk Management Guidance*.)

Any change that could have safety consequences in the provision of air traffic service is documented. The scale of an SRMD varies depending upon the type and complexity of a proposed system change.

The level (i.e., national, regional, or local) at which the SRM is initiated may vary by organization or change proponent. Safety significant changes at regional or local levels can employ two methods for documenting SRM:

1. address regional or local change in a system-wide SRMD through site-specific parameter ranges
2. develop and append a local-level SRMD to the larger, system-wide SRMD

A template and guideline information regarding the development of SRMDs can be found in Appendix D.

5.4 *What are the benefits of an SRMD?*

A standardized SRMD approach:

- reduces omissions and inconsistencies in safety risk assessment preparation
- eases documentation development
- makes sharing of safety risk data more manageable
- strengthens SRM skills
- encourages a safety culture
- ensures operational safety data are monitored to reduce hazards
- provides assurance to decision-makers that SMS processes are being followed
- establishes responsibility and accountability
- makes the process repeatable and reduces re-study of similar change proposals

5.5 *What is the difference between risk acceptance and SRMD approval?*

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

Approving the SRMD means that the approving party agrees that the analysis accurately reflects the safety risk associated with the change, the underlying assumptions are correct, and the findings are complete and accurate.

Both are necessary before a change is implemented in the NAS.

5.6 *Who approves the SRMD?*

The approvals in SRM (including approval of SRMDs) are dependent on the span of the program, its associated risk, and the mitigation(s) used to control the risk. In general, the person who approves the SRMD certifies that the documentation was developed properly, hazards have been systematically identified, and the risk has been appropriately estimated and mitigated. This approval *does not* constitute acceptance of the risk associated with the change or approval to implement the change. Specific approval requirements are described in Table 5.1.

In addition, it is important to get the approving authority involved early in the SRM process to get agreement on the assumptions and processes that will be used.

Table 5.1 - Safety Risk Management Approval Requirements

By AOV	SRMD Approved by ATO Safety Service Unit	SRMD Approved at the Service Director/Manager Level
<ul style="list-style-type: none"> • Safety Management System (SMS) processes and changes to SMS processes (as defined in this manual) • Changes to provisions of ATO documents related to separation minima (including waivers) • Controls used by ATO to mitigate hazards with high initial safety risk 	<ul style="list-style-type: none"> • Items or changes that require AOV approval • Any change that has high initial safety risk • Changes to, or replacement of, a system that if lost or malfunctioning would require application of contingency procedures involving increased separation standards or would result in "ATC Zero" status (e.g., ATOP or C-ARTS) • Changes in the periodicity of maintenance or inspection (including flight inspection) of systems described above (in 3rd bullet) 	<ul style="list-style-type: none"> • Changes with medium or low initial safety risk, where safety risk and controls/mitigations: <ul style="list-style-type: none"> ○ stay within ATO Service Unit, the SRMD is approved within the Service Unit ○ span ATO Service Units, the SRMD is approved within each affected Service Unit ○ go outside of ATO (i.e., to ARP and/or AVR), the SRMD is approved by each affected LOB

5.7 *What is AOV's role in SRMD approval?*

Unlike in the acceptance of risk, AOV does have a role in the approval of some SRMDs. The left-hand column in Table 5.1 describes AOV's role. AOV will approve SRMDs for proposed changes to SMS processes, as described in this manual, as well as proposed changes to provisions of ATO documents related to

separation minima (including waivers). In addition, AOV must approve the controls or mitigation strategies employed to reduce the safety risk of hazards with high initial risk to an acceptable level (low or medium). This is not the same as approving the SRMD.

All items that will go to AOV will first require approval of the ATO Safety Service Unit.

5.8 *What is the ATO Safety Service Unit's role in SRMD approval?*

The ATO Safety Service Unit does have a role in the approval of some SRMDs. The middle column in Table 5.1 describes its role. All items that will go to AOV will first require approval of the ATO Safety Service Unit. Any change that has a hazard with high initial risk will require Safety Service Unit approval of the SRMD before the mitigation strategies/controls are sent to AOV for approval.

In addition, any change to, or replacement of, a system that if lost or malfunctioning would require application of contingency procedures involving increased separation standards or would result in "ATC Zero" status (the complete lose of control services) requires ATO Safety Service Unit approval, as do changes in the periodicity of maintenance or inspection (including flight inspection) of those systems.

5.9 *What is the Safety Manager's and SSE's role in SRMD approval?*

If the risk must be approved at a high level within the service unit (certainly at the VP-level, but possible below), the Safety Manager will approve the SRMD. In addition, if the SRMD must go outside the service unit for approval (to another operational service unit, LOB, the Safety Service Unit, or AOV), the Safety Manager will approve the SRMD before it leaves the service unit.

The Safety Manager and/or Senior Safety Engineer (SSE) are also available to provide input to the management officials(s) who will accept the risk associated with the change.

5.10 *Once approved, where does the SRMD go?*

The change proponent retains a copy of the SRMD for a period equivalent to the lifecycle of the system or change. Upon request, the ATO Safety Service Unit is provided with copies of SRMDs.

SRMDs may also be inputs to existing approval processes (e.g., NAS Change Proposal (NCP) process, Document Change Proposal (DCP) process, etc.).

5.11 *What do I do with the SRMD if it is not approved, or if the change was not implemented?*

The SRMD should still be kept on file. This information will be useful in assessing similar change proposals or could be used as inputs to SRMDs for other change proposals. SRMDs that were not approved or those used by a decision-maker to choose not to implement a change also provide proof that the SMS is performing its intended function, reducing the safety risk in the NAS. This documentation is also auditable by the Safety Service Unit or AOV.

5.12 *How is an SRMD a living document?*

The results of risk assessment form part of the system baseline information. An SRMD may need to be updated or changed as a project progresses and decisions are modified. Safety monitoring may reveal less effective controls or greater than expected hazards. Any change that may affect the assumptions or hazards identified in the SRMD or that may affect the estimated risk necessitates an amendment to the SRMD.

The amended SRMD is denoted as such, is approved, and retained, as described above.

5.13 *Is there an acceptable substitute for an SRMD?*

In many instances, existing acquisition and system engineering processes produce documents that are compatible with, or could even be acceptable substitutes for an SRMD. The FAA *Acquisition System Toolset* (<http://fast.faa.gov/>) includes safety management guidance documentation and templates for each stage of the AMS lifecycle. Many of the FAA Handbooks already address safety aspects of specialty engineering, and many of the current system safety engineering processes result in documents compatible with the objectives or elements of an SRMD (e.g., *Operational Safety Assessment (OSA)*, *Comparative Safety Assessment (CSA)*, *System Safety Assessment Report (SSAR)*, etc.).

If an approved Agency process is already in use that complies with the requirements of Chapter 4, *Safety Risk Management Guidance*, and contains the necessary elements of an SRMD, the output of that process may be substituted for the SRMD (provided that the documentation complies with all approvals, document retention, and forwarding requirements set forth in this manual). Appendix D provides an SRMD template and additional guidance.



Chapter 6 – Safety Assurance and Evaluation

6.1 *Why safety assurance and evaluation?*

An essential function of the SMS is ensuring that safety objectives have been met. Safety assurance includes monitoring (i.e., safety reviews, evaluations, audits, and inspections), data tracking and analysis, and investigations. This chapter describes the monitoring function. Chapter 7, *Safety Data Tracking and Analysis*, details the FAA's use of safety data, investigations, and resulting outcomes.

Audits and evaluations can be defined as scheduled, formal reviews, examinations, and verifications of activities and operations. They improve the quality of products, processes, or services and provide a means for ensuring compliance with policy and/or contractual requirements. Audits also provide a means for evaluating the effectiveness of the overall program, identifying areas in need of improvement, and verifying the results of those improvements. The scope of auditing required varies with the stage of the program, its maturity, type of safety processes, and level of confidence developed from previous audits. Finally, audits contribute to the identification of deteriorating safety trends, which can lead to identification and mitigation of hazards.

Currently, many FAA organizations carry out essential safety auditing programs, some of which are described below. These current capabilities are an integral part of the SMS.

6.2 *What is a monitoring program?*

The monitoring program ensures compliance with SMS requirements, as well as FAA orders, standards, policies, and directives. Monitoring includes the following:

- safety reviews conducted in accordance with FAA Orders 7010.1, *Air Traffic Evaluations*; 7210.56, *Air Traffic Quality Assurance*; 6000.15, *General Maintenance Handbook for Airway Facilities*; 6040.6, *Airway Facilities NAS Technical Evaluation Program*; and 6000.30 *NAS Maintenance Policy*; and 8200.1, *United States Standard Flight Inspection Manual*
 - audits of the SMS processes, procedures, and outcomes
-

6.3 *What does a monitoring program involve?*

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

Physical Examination (PE) – is the activity of gathering physical evidence. This is a substantive test involving the counting, inspecting, gathering, and inventorying of physical and tangible assets such as cash, plants, equipment, parameters, etc.

Confirmation – is the act of using a written response from a third party to confirm the integrity of a specific item or assertion.

Vouching – is the examination of documents that support a recorded transaction, parameter, or amount. Testing starts with the recorded item and moves on to review the supporting documentation.

Tracing – is the following of source documents to their recording in the accounting records. This is a “through the system” method of accounting transaction flows, “ledgering” accounts, or logging parameters.

Reperformance – is an auditing technique of repeating a client process or activity with high fidelity and comparing results with previous operational data.

Observation – is the process of witnessing physical activities of the client. It differs from the PE in that the auditor observes the client performing the client’s process rather than the auditor performing the examination.

Reconciliation – is the process of matching two independent sets of records. The key here is independent. A derived set of data from the client does not meet this criterion, only third party or certified independent data meets the criteria. This satisfies the test of completeness and existence of evidence.

Inquiry – is the technique of “asking questions” and recording the response.

Inspection – is the critical examination of documents (different from vouching or tracing) to determine content and quality of a

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

transaction such as inspecting leases, contracts, minutes of meetings, requirements, client policy, etc.

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

FAA financial or programmatic assessments, fall into three categories of audits: financial audits, operational audits, and compliance audits.

Financial audits examine accounting and reporting of financial transactions. The purpose of this type of audit is to verify that there are sufficient controls and processes for the acquisition and use of resources.

The operational audit addresses the effectiveness and efficiency of the organization. The objective is to determine the organization's ability to achieve its goals, objectives, and mission.

The compliance audit is an evaluation or assessment of conformance to established criteria, process, or work practice. The objective is to determine if employees and processes have followed those policies and procedures established by management.

FAA organizations currently use both operational and compliance audits at the national and operating unit level to ensure quality.

The ATO Safety Service Unit will primarily use compliance audits to monitor the use of and overall effectiveness of the SMS, with a particular focus on SRM.

6.4 *Who is responsible for the assurance programs?*

The ATO has internal national monitoring and assurance programs, which evaluate the ATC units and equipment. In addition, each facility has a quality assurance advocate who is responsible for assurance at the facility-level.

The ATO Safety Service Unit audits SRM processes and outputs, as well as monitors the effectiveness of using safety data to identify and address deteriorating safety trends impacting the provision of ATC and navigation services. This is further described in Section 6.14.

- 6.5 *What does the current ATC facility monitoring program involve?*
- The current monitoring program is described in FAA Orders 7010.1, *Air Traffic Evaluations*, and 7210.56, *Air Traffic Quality Assurance*. The program includes evaluations and audits that have both a quality and a safety perspective.
- National evaluations are risk and capacity targeted, which means that the facilities with the most identified issues and greatest throughput, receive more frequent review than those that have fewer issues and/or low traffic volume. Special evaluations are also scheduled based on error data analysis.
- The evaluation team utilizes a standard checklist (documented in appendices to FAA Order 7010.1, *Air Traffic Evaluations*) for evaluation and audits to ensure that the full range of facility requirements are reviewed and rated. The items on the checklist are linked to existing FAA Orders, to which the facility is required to adhere.
-
- 6.6 *What is the difference between an evaluation and an audit of an ATC unit?*
- Evaluations are performed on site, while audits are an offsite method for assessing the facility. Audits are accomplished through discussions with facility personnel, and/or review of requested tape recordings, data, and documentation.
-
- 6.7 *How are ATC unit evaluations conducted?*
- Evaluations are accomplished through direct observation, data monitoring, attendance at personnel meetings, observation of training activities, review of administrative and maintenance records and reports, and interviews or discussions. Interviews involve many of the following: managers, supervisors, support and technical specialists, union representatives, employee participation group representatives, and other facility personnel.
-
- 6.8 *What happens after an ATC unit evaluation or audit?*
- Findings and issues are briefed to the unit management for development and prioritization of resolution strategies. Findings and issues are also tracked to resolution by the evaluating authority.
- Each item on the checklist is given a rating during the evaluation or audit. Items identified as problems, are brought to closure within 180 days. The process involves three steps:
- Corrective action - prescribes the actions to address the problem(s)
 - Follow-up action - validates that the action(s) solved the problem

- Management control is the action and/or program that remains in place to ensure that the issue does not recur

Follow-up evaluations are scheduled when warranted to ensure issues have been resolved in a timely manner. The identified issues are also reviewed in detail at the next scheduled evaluation to ensure that management control is effective.

6.9 *What are the outcomes of the ATC unit monitoring program?*

Reports are generated as a result of the evaluations, audits, and inspections. The reports are reviewed by the management authority, which has the ability to make changes to address identified concerns. In addition, these reports are reviewed by management above the level that is accountable for the area of concern. The purpose of the review is to identify, prioritize, and implement safety enhancing measures. This information is also tracked and analyzed for trends and to target future evaluations, audits, and inspections.

6.10 *What do the equipment monitoring programs involve?*

The equipment monitoring programs are described in FAA Orders 6000.15, *General Maintenance Handbook for Airway Facilities*; 6040.6, *Airway Facilities NAS Technical Evaluation Program*; and 8200.1, *United States Standard Flight Inspection Manual*.

The NAS Technical Evaluation Program (NASTEP) is the main component in the overall evaluation of maintenance activities. The NASTEP provides for independent review of four major program areas:

- how well facilities and services meet their intended objectives (functional as well as safety)
- how well the maintenance program is executed
- how well assets are managed
- how well customer needs are being met (including safety)

Essential elements of the NASTEP include:

- independent review of services provided
- reporting deviations from standards, technical problems, or deficiencies
- monitoring program status, progress, and responsiveness
- providing a mechanism for program and management feedback
- identifying, defining, and reporting anticipated critical problems
- improving the safety and operation of NAS facilities

The NASTEP provides the following:

- periodic independent technical review of services provided by system, subsystem, and equipment
- review of how well the services match customer needs
- on-site in-depth technical inspections by NASTEP evaluators including review of:
 - a. maintenance logs
 - b. technical performance records
 - c. Facility Reference Data File (FRDF)
 - d. required maintenance handbooks
 - e. aircraft accident reporting procedures
 - f. certification intervals
 - g. certification and key performance parameters

Many NAS facilities have performance characteristics that can only be measured or validated by airborne measurements. The FAA maintains a fleet of flight inspection aircraft specially equipped with high quality avionics equipment and position-determining systems to make these measurements. Most flight inspection activities occur on a periodic basis throughout the lifetime of a facility; commissioning and special inspections are also conducted. The flight inspection is detailed in FAA Orders 6000.15, *General Maintenance Handbook for Airway Facilities*; and 8200.1, *United States Standard Flight Inspection Manual*.

6.11 *How are evaluations conducted in the NASTEP?*

The NASTEP shifts the focus from inspection to evaluation. This, in turn, shifts the emphasis from just a “facilities” look to the broader emphasis on investigations and audits as a larger holistic approach to facility evaluations. The strategy is an incorporation of a collaborative Systems Management Office (SMO) and region-wide quality management methodology of system evaluation.

Specific evaluation techniques involve a two-step process. Step one, completed on 100 percent of the facilities, is to solicit and analyze data on compatible and associated groups of facilities and services. Based upon this first look, a prioritized list of facilities to be visited is generated. Step two is a site visit involving an in-depth wall to wall, floor to ceiling evaluation. The evaluations include information that is relevant to managerial decisions relating primarily to facility performance improvement and customer support.

The NASTEP program employs three basic types of evaluations:

- facility technical inspections
- facility group technical evaluations
- facility technical investigations

Assigned groups conduct most facility and services evaluations. All facilities are to be evaluated on a 4-year cycle with a nominal percent accomplished each year.

6.12 *What happens when issues are identified during an evaluation?*

All evaluations and findings reflect conditions as-found and are categorized into one of four types:

- **Critical Issue.** An issue that adversely affects an advertised service, has a substantive detrimental impact on the user, or clearly compromises safety.
- **Significant Issue.** An issue that has the potential to become critical, affects an advertised service, has a negative impact on the user, or could substantially improve service, etc.
- **Pending Issue.** An issue identified during the course of an evaluation, which requires additional investigation.
- **Information Only Issue.** All issues other than critical, significant, or pending issues.

Each critical finding requires closure in a timeframe from immediate to not more than 30 days. Each significant finding must be closed within two years. Pending and informational findings are categorized in the final evaluation report.

After the findings are defined and reported, the information is forwarded to a regional database where it is used to generate specific quarterly and annual reports. The database also supports various ad hoc queries as well as basis for special investigations. Reports are analyzed for trends and forwarded to the national program office for inclusion in national analysis and special investigations.

Group technical evaluations are conducted on nine types of groups comprised of interrelated facilities and services, which together provide services to pilots and air traffic controllers. Facility technical inspections are performed at a specific facility and are typically conducted during post-accident investigations upon request by regional or SMO management, or as required by national orders or directives. Facility technical investigations are in-depth inspection efforts. They are generally conducted by examining any or all characteristics of a particular facility or service, and are usually corrective in nature. Finally, “poor performer” investigations are conducted as a result of national analysis identifying facilities or services that warrant special or specific focus.

6.13 *What happens after an evaluation?*

Post audit or evaluation tasks are followed by a formal outbrief of findings and the issuance of an evaluation report. Findings are categorized as to the level of criticality and entered into the national database. Trends are analyzed and causal factors identified for further analysis and appropriate action. Action offices are designated for compliance and periodic reporting of status and progress in closing the identified issues.

6.14 *How is the SMS evaluated or audited?*

In addition to the evaluations, audits, and inspections described above, the overall effectiveness of the SMS is evaluated. As further described in Chapter 7, *Safety Data Tracking and Analysis*, safety data are tracked and analyzed for adverse trends and to identify the need for safety enhancing measures. Since the goal of the SMS is to increase the safety of the NAS by meeting or exceeding safety objectives, the SMS is evaluated on the FAA's ability to manage the safety risk in the NAS and meet these objectives.

The ATO Safety Service Unit also audits SMS processes and outcomes. Primarily using compliance audits, the office:

- reviews and provides input on safety risk assessments
 - reviews and provides recommendations regarding safety risk management processes and SRMDs
 - reviews and provides input on the results of safety assurance functions within FAA organizations
 - reviews safety data analysis reports
 - analyzes safety data and advises senior ATO and FAA management on safety related issues
-



Chapter 7 – Safety Data Tracking and Analysis

7.1 *Why collect and evaluate safety data?*

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

The safety data are used to:

- assess the effectiveness of training
- identify risks and verify the effectiveness of implemented controls
- identify areas where safety could be improved
- contribute to accident and incident prevention

7.2 *What is the ATO Safety Service Unit's role in the collection and analysis of safety data?*

The ATO Safety Service Unit leverages safety data that is available through various sources within and outside the Agency. The office analyzes safety data to identify adverse trends and identify indicators of potential safety issues. Over time, the data will help identify early indicators that point to potential problems in the system. Safety data are also used to assess the effectiveness of the SMS through tracking safety metrics. The office produces reports regarding NAS safety.

7.3 *What are the existing collecting and reporting processes for safety data?*

Currently, the FAA collects and reports safety data from a wide range of sources in the NAS. Table 7.1 (Section 7.13), lists many of the existing FAA Orders, processes, and databases related to safety data collection and reporting.

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

The reporting on serviceability of ATO facilities and systems, such as failures and degradations of communications, surveillance and other safety significant systems, and equipment is covered by FAA Order 6040.15, *NAS Performance Reporting System*, and Order 6000.30, *National Airspace System Maintenance Policy*. Maintenance guidelines, directives, checklists, configuration

management, and the NAS Technical Evaluation Program (NASTEP) contribute to the periodic reviewing and maintenance of equipment and procedures.

The *Safety Recommendation Reporting System* provides a method for FAA Aviation Safety Inspectors to develop and submit safety recommendations directly to the Office of Accident Investigation (Order 8020.11 *Aircraft Accident and Incident Notification, Investigation and Reporting*).

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

The Unsatisfactory Condition Report (UCR) program (FAA Order 1800.6, *Unsatisfactory Condition Report*) "provides all Agency employees with a direct and simple means of advising management of unsatisfactory conditions."

7.4 *What is the process for reporting safety incidents and accidents?*

When an incident occurs, it is reported to ATO Systems Operations Service Unit in a *Preliminary Operational Error/ Deviation Investigation Report* within three hours. Within 1 hour of receiving the report, the event is scored according to risk. The scores range from A to D (A - being severe risk to D - being low risk). The preliminary report and the preliminary risk score are finalized into a *Final Operational Error/ Deviation Report* within 45 days.

In the case of surface incidents, the data are forwarded to the Runway Safety Directorate within the Safety Service Unit, and authorities score the event based on the severity of the incident. Similar to airborne events, a score of A to D is applied, and a report is produced and made available within 1 week of the event.

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

In cases where a pilot deviation is identified, the Flight Standards District Office (FSDO) is informed, and it investigates the event to determine what further action to take.

The incident reporting process is depicted in Figure 7.1.

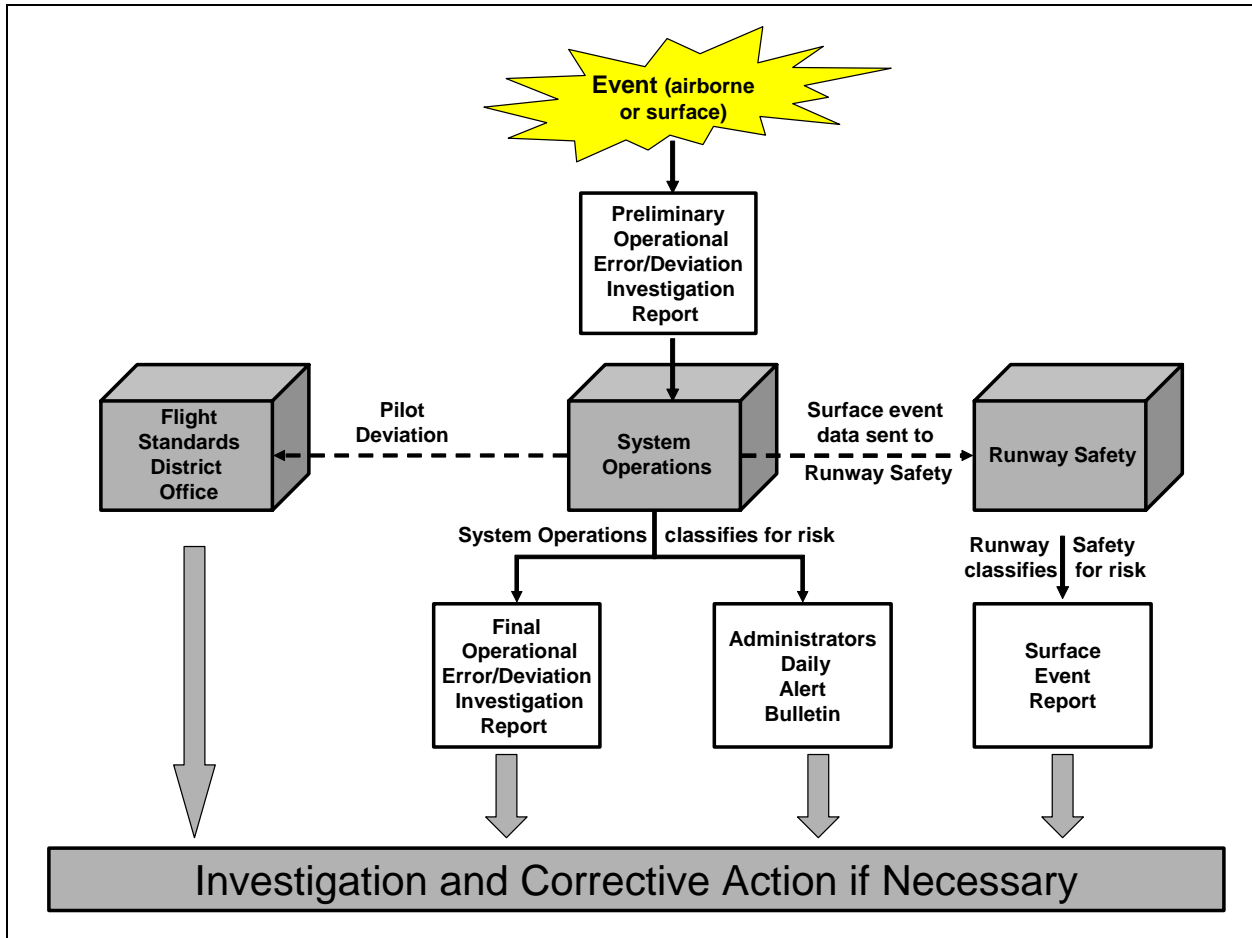


Figure 7.1 - Incident Reporting

7.5 *How does incident reporting enhance safety?*

Event reporting leads to investigations. During an investigation, the event is reconstructed and analyzed. During the reconstruction, contributors to the event are identified. Contributors are characterized as either direct or indirect. Factors that may have lessened the impact of the occurrence are also identified. All of these factors are analyzed for risk and often relate to the SRM process. The contributing factors and risk characteristics are used as inputs to develop recommended mitigation strategies and safety enhancing measures to preclude similar events in the future.

Corrective action to enhance safety is implemented at all levels, from national to local, and data are continuously tracked to identify improvement or degradation trends.

Data is reviewed and trended, which may lead to:

- airspace and airport improvements
- additional communications, navigation, or surveillance (CNS) systems and/or automation systems
- additional staffing
- other safety enhancing changes

7.6 *How is incident investigation related to hazard analysis (and SRM)?*

Experience has shown that for every catastrophic accident there are many precursor incidents or minor accidents. For each incident, there are numerous precursor hazards. There are organizations that have mature processes to investigate accidents (i.e., National Transportation Safety Board (NTSB), FAA Office of Accident Investigation (AAI), etc.) and conduct analyses that proactively look for potential hazards. However, accident prevention programs focus on the collection, analysis, and investigation of incident data.

Incident investigation is valuable because of two critical characteristics:

- it reflects real-world occurrences
- if adequately collected, the information about the incident is intact and not destroyed

The SMS requires the collection and analysis of incident data to determine if hazards exist, and to manage the risk of those hazards with the intent of preventing future accidents. The key is developing the capability to sort and analyze the vast array of data and transform it into useful information that permits the identification of hazards. Once this is done, the hazard can be managed in the same manner as any other identified hazard.

7.7 *What safety data are reported regarding serviceability of equipment, systems, and facilities?*

The majority of daily system performance metrics (including incident reporting) are captured via the outage reports, significant event reports, and general maintenance logging. Additional reports are made in the form of Notice to Airmen (NOTAMS), and accident reporting. Additionally, data are collected via a formal hotline and through the UCR program. Outage and incident data are consolidated into a daily report for the Office of the Administrator.

- 7.8 *How does serviceability reporting enhance safety?*
- Equipment installed in the NAS used for aircraft separation has established performance metrics used for system safety. The monitoring of overall trends and performance levels is accomplished systematically and documented via its certification. "Certification is a quality control method used to ensure NAS systems and services are performing as expected" (FAA Order 6000.30C, paragraph 11d).
- The NASTEP and UCR programs require written documentation, as well as management involvement in the review, mitigation, and analysis of trends.
- Through the NASTEP, periodic independent technical reviews of services provided by system, subsystem, and equipment are conducted. These reviews also address how well the services match customer needs.
- 7.9 *What data are reported?*
- The processes listed above describe reporting of specific types of safety data. However, over and above the reporting of these data, it is important that each employee reports any occurrence or situation that he or she thinks is, or could become, a hazard within the NAS.
- 7.10 *Where do I report safety concerns?*
- FAA staff should report safety concerns to their supervisors. In such cases, supervisors require employees to document as much information as possible about the concern. Where the type of safety issue being reported is covered by an existing FAA order, the procedures outlined in that order are followed.
- 7.11 *If current reporting processes are not applicable, how do I report a safety hazard?*
- In the case where none of the orders or programs apply to a particular safety concern, employees should report the issue to their immediate supervisor. If the supervisor deems it necessary, the issue is reported to the ATO Safety Service Unit for analysis. Feedback on the outcome of the analysis is provided to the supervisor reporting the concern.
- 7.12 *Where is the safety data stored?*
- Several aviation safety databases are populated with information regarding the safety events and the serviceability of the NAS. Several of the databases are described in the following paragraphs.
- Safety events are collected and categorized in the National Aviation Information Management System (NAIMS) database. The Systems Operations Service Unit maintains a database that provides severity classifications for airborne operational errors.

The Runway Safety Directorate categorizes surface events that include surface operational errors, operational deviations, pilot, vehicle, and pedestrian deviations. AAI investigates and tracks aircraft accidents and publishes monthly reports.

Pilot deviations are reported by air traffic facilities, reviewed by Systems Operations for air traffic involvement, and investigated and tracked by Flight Standards.

Near midair collisions are reported to air traffic facilities by flight crews, are reviewed by Systems Operations for air traffic involvement, and are investigated and tracked by Flight Standards. The data are stored in Near Midair Collision System (NMACS) database.

The National Aviation Safety Data Analysis Center (NASDAC) enables integrated queries across multiple databases, allowing users to search the warehoused safety data and display queries in useable formats.

7.13 *What are other ways safety data are used to improve the safety of the NAS?*

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

- NTSB recommendations
 - requirements for new CNS and/or automation services to enhance or expand airspace management
 - unsatisfactory reports (as discussed above)
 - employee suggestions
 - applications for procedural changes
 - research and development
 - acquisition of new systems (hardware and software) and equipment
 - industry advocacy
 - participation in international forums
-

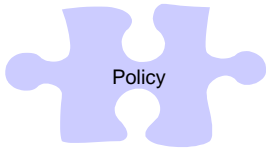
Table 7.1 - Safety Data Reporting Documents and Processes

<i>FAA Orders and Processes Related to Safety Data Reporting</i>		
Type of Data	Overview	References
Mandatory Reporting Data		
Air traffic incidents	This order mandates that data concerning air traffic incidents is collected and analyzed.	Order 7210.56, <i>Air Traffic Quality Assurance</i>
Aircraft accident/incident	This order contains reporting requirements regarding safety issues, concerns, incidents, and accidents.	Order 8020.11, <i>Aircraft Accident And Incident Notification, Investigation, and Reporting</i>
System outages	This order mandates outage reports and contributes to the daily system performance and incident reporting.	Order 6040.15, <i>National Airspace Performance Reporting System</i>
Significant system events	This order mandates the reporting of significant events and contributes to the daily system performance and incident reporting.	Order 6030.41, <i>Notification Plan for Unscheduled Facility and Service Interruptions and Other Significant Events</i>
Unsatisfactory condition	This order provides Agency employees a means of advising management of unsatisfactory conditions.	Order 1800.6, <i>Unsatisfactory Condition Report</i>
Oceanic Altitude/Nav Errors	This order establishes procedures for processing reports and for collecting system data for analysis.	Order 7110.82. <i>Monitoring of Navigation, Longitudinal Separation, and Altitude Keeping Performance in Oceanic Airspace</i>
Safety Recommendations	This order establishes procedures for Aviation Safety Inspectors to report safety recommendations directly to the Office of Accident Investigation (AAI-100).	Order 8020.11 <i>Aircraft Accident and Incident Notification, Investigation and Reporting</i>
National Aviation Safety Data Analysis Center (NASDAC)	The NASDAC system enables users to perform queries across multiple databases and display queries in useful formats.	The NASDAC is a data warehouse and integrated database system.
National Aviation Information Management System (NAIMS)	A database where safety events are collected and categorized.	
Runway Safety Directorate within the Safety Service Unit	The Runway Safety Directorate categorizes surface events that include surface operational errors, operational deviations, pilot, vehicle, and pedestrian	

<i>FAA Orders and Processes Related to Safety Data Reporting</i>		
Type of Data	Overview	References
	deviations.	
Accident/Incident Reporting Data System (AIDS)	The FAA AIDS database contains accident and incident data records for all categories of civil aviation.	
NTSB Accident/Incident Database	The NTSB accident/incident database is the official repository of aviation accident data and causal factors. In this database, events are categorized as accidents or incidents.	
Operational Error/Deviation System (OEDS)	Used by determine if actions of a controller resulted in a loss of separation or an aircraft landing or departing on a closed runway.	
Pilot Deviation System (PDS)	Used by FAA to determine if actions of a pilot violated regulations.	
Hazards related to the acquisition and implementation of new systems	Designed to identify, eliminate, or resolve determined or assigned risk, estimate a likelihood of occurrence, and track hazards throughout the life cycle of a program.	Hazard Tracking System, FAST Toolset, and the Acquisition Management System
Voluntary Reporting Data		
Aviation Safety Reporting System (ASRS) and Aviation Safety Reporting Program (ASRP)	ASRS and ASRP are voluntary programs designed to encourage the identification and reporting of deficiencies and discrepancies in the airspace system. The National Aeronautics and Space Administration (NASA) accomplish receipt, processing, and analysis of raw data rather than by the FAA, which ensure the anonymity of the reporter and of all parties involved in a reported occurrence or incident and, consequently, increase the flow of information necessary for the effective evaluation of the safety and efficiency of the system.	Advisory Circular 00-46, <i>Aviation Safety Reporting Program</i>
Aviation Safety Action Program (ASAP)	Voluntary reporting of safety issues and events that come to the attention of employees of certain certificate holders. To encourage an employee to voluntarily report safety issues even though it may involve an alleged violation of Title 14 of the Code of Federal Regulations (14 CFR), enforcement-related incentives	Order 1110.129, <i>Aviation Safety Action Program Aviation Rulemaking Committee</i> and Advisory Circular 120-66, <i>Aviation Safety Action Program (ASAP)</i>

<i>FAA Orders and Processes Related to Safety Data Reporting</i>		
Type of Data	Overview	References
	have been designed into the program.	
Near Midair Collision System (NMACS)	It is the responsibility of pilots and/or flight crew members to determine whether a NMAC actually occurred and, if so, initiate a NMAC report. There is, however, no regulatory or legal requirement that a pilot and/or flight crew report a NMAC event, although they are encouraged to do so.	Program is administrated by the Office of System Safety (ASY).
Global Aviation Information Network (GAIN) ¹⁴	The GAIN, an industry-led international coalition of airlines, manufacturers, employee groups, governments and other aviation organizations, was formed to promote and facilitate the voluntary collection and sharing of safety information.	Program is administrated by ASY.
Automatic Reporting Data		
Incident and maintenance reporting in Maintenance Management System (MMS)	The MMS contains general maintenance logging, which contributes to the daily system performance and incident reporting.	Order 6000.48, <i>General Maintenance Handbook for Automated Logging</i>

¹⁴ The Global Aviation Information Network (GAIN) program provided information on several of the data sources listed in Table 8.



Chapter 8 – SMS Responsibilities and Accountabilities

-
- 8.1 *Who is responsible for safety?* All FAA employees, managers, and contractors who are either directly or indirectly involved in the provision of ATC or navigation services are responsible for the safety of the NAS. Each individual is responsible for the safety of his/her actions. Each individual is responsible for communicating relevant safety-related information and giving the highest priority to providing the safest possible NAS.
-
- 8.2 *ATO Chief Operating Officer* The ATO Chief Operating Officer (COO) has accountability for the safety of the NAS and the implementation of the SMS.
-
- 8.3 *Vice President (VP) for Safety in the ATO* The VP for Safety is accountable for the following:
- leading the ATO Safety Service Unit
 - promoting and strengthening the FAA safety culture
 - advising the COO on the SMS and safety-related issues
 - implementing, maintaining, and evaluating the SMS
 - being the primary ATO interface with AOV
-
- 8.4 *ATO VPs, Managers, and Supervisors* All ATO VPs, managers, and supervisors are accountable for the implementation of, and adherence to, SMS policies and procedures within their span of control. Two fundamental responsibilities are:
- accepting the risk associated with NAS changes
 - reinforcing a safety culture in their organizations
-
- 8.5 *NAS Change Agents* NAS change agents are responsible for conducting safety risk management on safety significant NAS changes. Two fundamental responsibilities are:
- documenting decisions to either employ, or not employ SRM when implementing changes in the NAS
 - monitoring and maintaining a list of hazards and mitigation measures (i.e., hazard tracking)
-
- 8.6 *Safety Manager (in operational service units)* Each operational service unit/organization will designate a Safety Manager who will be the focal point for safety within the organization. The Safety Manager's responsibilities include:
- conducting service unit safety planning and monitoring
 - ensuring that the service unit meets SMS requirements

- providing support/consultation on safety management within service unit
 - approving certain SRMDs
 - facilitating intra-service unit coordination on safety
 - providing input and advice on safety to VP
-

8.7 *Senior Safety Engineers (in operational service units)*

Each service unit/organization will have a Senior Safety Engineer (SSE) who will report to the Safety Manager and will provide safety risk management technical expertise within the service unit. The SSEs responsibilities include:

- supporting, advising, and assisting programs and analysis teams in conducting SRM activities
 - facilitating, if needed, SRM decision process and resulting documentation
 - providing recommendations to Safety Manager on SRMD approval
 - providing input to service unit VP, managers, and directors on risk acceptance
 - providing input and advice on safety to VP and Safety Manager
-

8.8 *Associate Administrator for Airports*

The Associate Administrator for Airports (ARP) is accountable for the following:

- safety functions within ARP that impact ATC and navigation services
 - implementation and compliance of the SMS policies and procedures within ARP as ARP impacts NAS safety
-

8.9 *Associate Administrator for Office of Regulation and Certification*

The Associate Administrator for Office of Regulation and Certification (AVR) is accountable for the following:

- safety functions within AVR that impact ATC and navigation services
 - implementation and compliance of the SMS policies and procedures within AVR as AVR impacts NAS safety
 - safety oversight of the ATO through AOV
-

8.10 *Director of the Air Traffic Safety Oversight Service*

The Director of the Air Traffic Safety Oversight Service (AOV) is accountable for overseeing ATO safety. For more information regarding AOV, see Chapter 11, *Safety Oversight*.



Chapter 9 – SMS Training Standards

9.1 *Who receives training?*

Employees receive information and training in SMS concepts, processes, and procedures at a level that is commensurate with their job functions as they relate to the SMS. To that end, in addition to communications providing an overview and awareness of the SMS concepts and processes, two levels and types of training is provided.

Training that facilitates the use of SMS outputs in decision-making is provided for ATO executives, directors, and managers. In addition, practitioners receive detailed training on the elements of SRM. The training includes an introduction to the tools to be used.

However, it is recognized that SRM in an operational environment differs from the analysis and tools used in assessing new systems or changes to existing systems (hardware and software). Therefore, the specific tools are taught in modules as add-ons to the practitioner course to ensure that training is efficiently targeted.

9.2 *What training is provided?*

- SMS Executive and Manager training
- SRM Practitioner training (with SRM Tools modules)

9.3 *Who develops and provides training?*

The ATO Safety Service Unit is primarily responsible for developing and facilitating the delivery of SMS training. To do so, the office will leverage existing safety management training.

9.4 *Who is the target audience of SMS Executive and Manager training?*

High-level support and understanding of the SMS, its concepts, and tools are critical success factors of the SMS. In addition to having a basic understanding of the SMS, decision-makers must understand how to use SMS outputs as inputs (from a safety perspective) to decision-making processes. The SRMDs, safety data analysis reports, and results of safety reviews allow management to make informed decisions and prioritize initiatives. Executives and managers must also understand when SRM is necessary. They must know when to elevate decisions and the supporting information to a higher-level.

9.5 *What topics are covered in SMS Executive and Manager training?*

SMS Executive and Manager training provides information on the components and uses of SMS outputs to support decision-making.

Topics include:

- SMS concepts, terms, and processes
- SMS accountabilities and responsibilities
- SRM concepts
- depth and breadth of safety data collected and analyzed
- understanding the process to determine when SRM is required
- using SMS outputs to support decision-making
- executive and manager SMS accountabilities
- strengthening the FAA safety culture

9.6 *How is SMS Executive and Manager training delivered?*

Multiple media is used to provide Executive and Manager training; including Computer-based Instruction (CBI), Web-based Instruction (WBI), satellite broadcast, and/or classroom training. However, initially classroom training will be the primary method employed.

9.7 *Who is the target audience of SRM Practitioner training?*

Understanding and use of SMS tools by employees making changes to the NAS are critical SMS success factors. SRM has been identified as the element of the SMS that has the greatest opportunity for enhancement in the FAA. In addition to having an understanding of the SMS and how SRM fits within it, practitioners must have in-depth knowledge of SRM tools, documentation requirements, development of mechanisms to monitor controls, and risk mitigation strategies developed during safety risk assessment.

SRM Practitioner training is required for employees who conduct safety risk assessments and/or those responsible for any component of SRM when making changes to the NAS.

9.8 *What topics are covered in SRM Practitioner training?*

SRM Practitioner training provides detailed information on SRM, and its uses, tools, and documentation requirements.

Topics include:

- SRM concepts and terms
- SRM processes, to include how they relate to existing processes (Acquisition Management System, T&E Gold Standard, etc.)
- SRM tools, to include recommended tools for a variety of changes

- identifying when SRM is required
- documentation requirements for changes
- development of SRMDs
- development of controls and safety risk mitigation strategies
- development of monitoring mechanisms for controls and safety risk mitigation strategies
- understanding of risk acceptance and SRMD approval processes
- knowledge of when decisions need to be elevated or coordinated beyond the team or individual conducting the safety risk assessment

9.9 *How is SRM Practitioner training delivered?*

Multiple media are used for training; including CBI, WBI, satellite broadcast, and/or classroom training. However, initially classroom training will be the primary method employed.

9.10 *Who is the target audience of SRM Tools modules?*

In addition to having an understanding of the SMS and how SRM fits within it, practitioners must have in-depth knowledge of the SRM tools. These modules allow practitioners to build upon their knowledge of SRM and learn about the application of specific tools.

SRM in an operational environment differs from assessing new or modified systems (hardware and software). Training modules include appropriate tools to ensure that those involved in assessing and managing risk associated with NAS changes have the knowledge relevant to the types of changes that they make.

9.11 *What topics are covered in SRM Tools modules?*

The modules build upon the concepts covered in SRM training to provide more detailed information on specific tools. Topics include:

- strengths and weaknesses of the tool
- complementary tools that could be used to accommodate weaknesses
- mapping the outputs of the tool to development of SRMDs
- mapping the outputs of the tool to development of controls and safety risk mitigation strategies

9.12 *How are SRM Tools modules delivered?*

Multiple media are used to deliver SRM Tools modules; including CBI, WBI, and/or classroom training.

9.13 *Where can I get more information about SMS training?*

The ATO Safety Service Unit can provide more information concerning SMS training.



Chapter 10 – Safety Culture

10.1 *What is a safety culture?*

In this context, a safety culture refers to the personal dedication and accountability of individuals engaged in any activity that has a bearing on the safe provision of air traffic services. It is a pervasive type of safety thinking that promotes an inherently questioning attitude, resistance to complacency, a commitment to excellence, and the fostering of both personal accountability and corporate self-regulation in safety matters.

Safety culture then is both attitudinal as well as structural, relating to both individuals and organizations. It concerns the requirement to not only perceive safety issues, but to match them with appropriate action. Safety culture relates to such intangibles as personal attitudes and the style of the organization. It is therefore difficult to measure, especially when the principal criterion for measuring safety is the absence of accidents and incidents. Yet, personal attitudes and corporate style do enable or facilitate unsafe acts and conditions that are precursors to accidents and incidents.

Safety culture goes beyond mechanistic adherence to procedures. It requires that all duties important to safety be carried out correctly, with alertness, due thought and full knowledge, sound judgment, and a proper sense of accountability.

10.2 *What values are inherent in a safety culture?*

An organization's culture is defined by what the people do. Organizational values can be judged by decision-makers' actions. For instance, the extent to which managers and employees act on commitments to safety, demonstrates the values that motivate their actions. To foster a safety culture, senior management sets the standards by allocating adequate resources, providing unambiguous policy direction, and promoting open communication. Safety training is especially important activity for strengthening organizational safety culture.

The following values are inherent in a safety culture:

- people at all levels understand the hazards and risk inherent in their operations and those with whom they interface
- personnel continuously work to identify and control or manage hazards or potential hazards

- errors are understood, efforts are made to eliminate potential errors from the system, and willful violations are not tolerated
- employees and management understand and agree on what is acceptable and unacceptable
- employees are encouraged to report safety hazards
- when hazards are reported, they are analyzed using a hazard-based methodology, and appropriate action is taken
- hazards, and actions to control them, are tracked and reported at all levels of the organization
- employees are encouraged to develop and apply their own skills and knowledge to enhance organizational safety
- staff and management communicate concerning safety hazards openly and frequently
- safety reports are presented to staff so that everyone learns the lessons

10.3 *Why is a safety culture important?*

Developing the processes and procedures for an SMS is not enough to ensure that safety is actually enhanced by the system. A safety culture supports the tenets of the SMS since all employees understand their unique significance in the safety of the NAS. Safety is given the highest priority in any decision that is made, and every employee understands the safety consequences of his or her actions.

10.4 *What is a positive reporting culture?*

A safety culture is further reinforced by a positive reporting culture. An organization with a positive reporting culture is one in which:

- the reporting system is simple and user-friendly
- management encourages the reporting of safety occurrences
- the treatment of staff who submit safety reports is seen to be just
- each occurrence report received is investigated
- feedback is provided to the originator of the report
- management ensures that the submission of reports results in corrective action to prevent recurrence
- confidentiality is maintained, insofar as possible, in relation to disclosure of information concerning individuals
- lessons learned are disseminated to all staff personnel

10.5 *Why is it important to share safety data Agency-wide?*

Accidents and incidents are rarely caused by single events; rather they are a function of multiple events. In a system as large and diverse as the NAS, the numerous organizations that have responsibility for components of the NAS each have a different

and important perspective. These multiple events often fall in the purview of multiple organizations. Sharing safety data and analyses assists the FAA in identifying issues that are the result of events on which only one organization within the Agency would not normally focus.

Some of the databases (e.g. NASDAC and NAIMS) described in Chapter 7, *Safety Data Tracking and Analysis*, consolidate data from multiple sources allowing an Agency-wide perspective. The SMS supports further integration and sharing.

10.6 *Why is the dissemination of lessons learned important?*

The SMS is an evolutionary system that is constantly maturing. As the system matures, the processes will become more refined and more engrained into existing FAA processes and procedures. Dissemination of lessons learned will expedite the maturation process by identifying and resolving problems and issues rather than allowing them to repeat in perpetuity. Sharing lessons learned also fosters an FAA-wide perspective to decision-making, as well as improves the efficiency of both the maturation of the SMS and the NAS.

An important function of the Safety Service Unit is to facilitate the documentation, collection, and distribution of “lessons learned” from the implementation and utilization of the SMS.

10.7 *What impact can organizational factors have?*

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

10.8 *How does the SMS fit within the other safety programs in the FAA?*

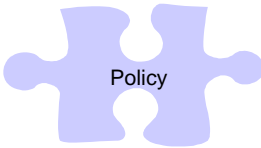
The SMS should not be viewed as a new system implemented in the name of safety. Instead, the SMS builds upon the processes and procedures that currently exist, such as the AMS processes, system safety engineering, testing and evaluation, facility auditing, equipment inspection, and many data collection and analysis systems. In some cases, existing processes and documentation may need to be more formalized to comply with the SMS. However, in many cases many of the existing processes fit within the SMS construct.

The SMS provides high-level visibility and commitment to the identification and mitigation of safety hazards. Also the SMS facilitates cross-organizational communication and cooperation by providing a common framework. All of this promotes the safety culture discussed above.

10.9 *What role does the ATO Safety Service Unit play in supporting the SMS and promoting the safety culture?*

The FAA has a strong safety culture. An important role of the ATO Safety Service Unit is to document and complement the current safety culture. The office assists the further development and strengthening of the safety culture by playing a vital role in the facilitation of cross-organizational communication and coordination, safety data sharing, and dissemination of lessons learned. It is the central repository of SMS information and knowledge, and a resource regarding the components of the SMS. The office also collects and disseminates lessons learned on safety and the SMS, and provides input from a safety perspective to decision-makers.

The ATO Safety Service Unit audits the SMS processes and outcomes to facilitate the evolution of the system. Finally, the office will develop subsequent versions of this manual and additional guidance materials (as required) to further strengthen and clarify the SMS.



Chapter 11 – Safety Oversight

11.1 *What is the purpose of FAA safety oversight?*

The FAA Administrator created the Air Traffic Safety Oversight Service (AOV) to provide independent safety oversight of the ATO. AOV is located within the Office of Regulation and Certification (AVR).

Per ICAO recommendations, “In those States where the Civil Aviation Authority (CAA) also acts as both the regulator and air traffic service provider, it is important that a clear separation between the air traffic service provision function and the air traffic service safety regulatory function be maintained. The safety regulation of the service provider should be conducted as though the service provider was an external entity in order to maintain the independence of the regulatory function.”¹⁵

11.2 *From where does AOV derive its authority?*

The FAA Administrator delegated authority to the Associate Administrator for Regulation and Certification to oversee the safety of the ATO. This authority is documented in the Air Traffic Safety Oversight Service Order, which describes AOV and ATO roles and responsibilities regarding NAS safety.

11.3 *What are AOV’s responsibilities and what authority does it have?*

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

- establish, approve, and/or accept safety standards for the operation and maintenance of the NAS
- establish the requirements for the SMS
- approve the SMS and any changes to the SMS
- monitor ATO compliance with the safety standards and the SMS
- audit ATO compliance with the safety standards and the SMS
- monitor corrective actions taken by ATO to assure resolution of identified safety hazards
- provide safety information to the FAA Administrator

¹⁵ Eleventh Air Navigation Conference, Montreal, 22 September to 3 October 2003, *The Manual on Safety Management for Air Traffic Services, Appendix – Draft Manual on Safety Management for Air Traffic Services*, Chapter 9, Section 9.1.5, p. A-185.

- issue safety directives, letters of correction, and/or warning letters to ATO if it deems such an action necessary/appropriate
- review, for concurrence, any proposed responses to safety recommendations from the National Transportation Safety Board (NTSB), the Office of the Inspector General (OIG), or General Accounting Office (GAO) involving ATO
- review, for concurrence, notifications of differences proposed to be filed by ATO with ICAO
- serve as the primary AVR interface with ATO on safety issues
- share safety data with ATO

11.4 *What is the difference between approval by AOV and acceptance by AOV?*

Approval by AOV is the formal act of approving a change submitted by a requesting organization. This action is required prior to the proposed change being implemented. See Section 11.5 for those items that require AOV approval.

While, *acceptance* by AOV is the process whereby AOV has delegated the authority to the ATO to make changes within the confines of approved standards and only requires the ATO to notify AOV of those changes. See Section 11.6 and 11.7 for those items that require AOV acceptance.

11.5 *What requires approval from AOV?*

The following items or changes require AOV approval prior to implementation:

- the SMS manual and proposed changes to the SMS manual
- controls that are defined to mitigate or eliminate initial high risk hazards (taking into account all existing controls)
- changes to any provisions of handbooks, orders, and/or documents that pertain to separation minima (including waivers)

11.6 *What requires acceptance by AOV?*

The following items or changes require acceptance by AOV:

- exclusions to SMS requirements granted by the ATO Safety Service Unit
- changes to the areas of FAA Order 8200-1, *United States Standard Flight Inspection Manual* stated below:
 - h. flight Inspector's authority and responsibilities
 - i. facility status classification and issuance of Notices to Airmen (NOTAMs)
 - j. records and reports
 - k. extensions in the periodicity or interval of inspections

- l. changes in established tolerances or those proposed for new equipment or new functionality
- m. changes in required checklist items for specific areas of systems to be inspected
- n. changes in the procedures for evaluating safety and flyability of instrument flight procedures
- changes to personnel certification requirements contained in Order VN 8240.3, *Certification of Flight Inspection Personnel*
- changes to the certification standards contained in Order VN 3330.2, *National Flight Procedures Office (NFPO) Certification Program for Procedures Personnel*
- changes to personnel certification requirements contained in FAA Order 7220.1, *Certification and Rating Procedures*
- changes to Certification Criteria in Order 6000.15, *The General Maintenance Handbook*, (in paragraph 504)
- changes to the personnel certification requirements contained in FAA Order 3400.3, *Airway Facilities Maintenance Personnel Certification Program*
- mitigations/controls in cases where safety risk and/or controls/mitigations go outside of the ATO (i.e. ARP and or AVR); the mitigations must also be approved by the designated management officials within each affected LOB

11.7 Does the establishment of AOV change AFS's role in the provision of ATC and navigation services?

No, for the most part, AFS's role remains the same. AFS still must approve the following items/changes, which also require acceptance by AOV:

- Changes to the areas of FAA Order 8200-1, *United States Standard Flight Inspection Manual* stated below:
 - o. Flight Inspector's authority and responsibilities
 - p. Facility status classification and Notices to Airmen (NOTAMs)
 - q. Records and reports
 - r. Extensions in the periodicity or interval of inspections
 - s. Changes in established tolerances or those proposed for new equipment or new functionality
 - t. Changes in required checklist items for specific areas of systems to be inspected
 - u. Changes in the procedures for evaluating safety and flyability of instrument flight procedures
- Changes to personnel certification requirements contained in Order VN 8240.3, *Certification of Flight Inspection Personnel*

- Changes to the certification standards contained in Order VN 3330.2, *NFPO Certification Program for Procedures Personnel*

11.8 *How does the ATO interface with AOV?*

ATO interface with AOV must be coordinated through the ATO Safety Service Unit. Similarly, AOV has agreed to coordinate all ATO interactions with the ATO Safety Service Unit.

11.9 *What will be different as the ATO makes the transition to a fully functional SMS?*

During transition to a fully functional SMS, if your organization has not received SMS training and is not yet operating under the purview of the SMS, then the following provisions apply:

- the change must be documented per the direction of the ATO Safety Service Unit (as described in Chapter 3)
- the change must be made in accordance with orders and operating practices in place immediately prior to SMS implementation
- waivers to safety standards, as described in Sections 11.5 and 11.6 in this manual and Section 4 of the Air Traffic Safety Oversight Service Order require AOV approval prior to implementation

11.11 *How can I get more information regarding oversight and the ATO's relationship with AOV?*

Contact the ATO Safety Service Unit for more information.

Appendix A – References to FAA Documents Related to SMS Requirements

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

In addition, in some cases the document listed below may have been updated since this list was compiled. Refer to the office of primary interest for the most recent version of the document.

General:

- Order 1220.2, FAA Procedures for Handling NTSB Safety Recommendations
- Order 1800.6, Unsatisfactory Condition Report RIS
- Advisory Circular No: 00-46: Aviation Safety Reporting Program (ASRP)

Airports:

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

Air Traffic Control:

- Advisory Circular 120-66, Aviation Safety Action Program (ASAP)
- Order 1100.2, Organization – FAA Headquarters
- Order 1110.129, Aviation Safety Action Program Aviation Rulemaking Committee
- Order 1800.14, Airway Facilities Management Consulting Evaluation Program
- Order 3120.4, Air Traffic Technical Training
- Order 3120.27, Performance Verification for En Route and Terminal Initial Qualification Training
- Order 6040.15, National Airspace Performance Reporting System
- Order 6050.19, Radio Spectrum Planning
- Order 6050.22, Radio Frequency Interference Investigation and Reporting
- Order 6050.32, Spectrum Management Regulations and Procedures Manual
- Order 6480.4, Airport Traffic Control Tower Siting Criteria
- Order 7010.1, Air Traffic Evaluations
- Order 7110.49, Unlawful Interference – Hijack/Bomb (Threat) Aboard Aircraft Procedures and Covert Signals
- Order 7110.82, Monitoring of Navigation, Longitudinal Separation, and Altitude Keeping Performance in Oceanic Airspace
- Order 7110.112, Simultaneous ILS/MLS Blunder Data Collection

- Order 7210.3, Facility Operation and Administration
- Order 7210.56, Air Traffic Quality Assurance
- Order 7210.58, National Runway Safety Program
- Order 7220.1, Certification and Rating Procedures
- Order 7400.2, Procedures for Handling Airspace Matters
- Order 7610.4, Special Military Operations
- Order 7900.2, Reporting of Electronic Navigation Aids and Communication Facilities Data to the NFDC
- Order 7910.3, Position Display Map Program
- Order 7930.2, Notices to Airmen (NOTAMS)
- Order 8020.11, Aircraft Accident and Incident Notification, Investigation and Reporting

Facilities & Equipment:

- Order 1320.58, Equipment and Facility Directives – Modification and Maintenance Technical Handbooks
- Order 1800.66, Configuration Management Policy
- Order 1900.47, Air Traffic Services Contingency Plan
- Order 3000.10, Airway Facilities Maintenance Technical Training Program
- Order 3400.3, Airway Facilities Maintenance Personnel Certification Program
- Order 3900.19, Occupational Safety and Health Program
- Order 4140.1, Integrated Material Management Program
- Order 4441.16, Acquisition of Telecommunications Systems, Equipment, and Services
- Order 4630.5, Quality and Reliability Assurance of General Operating Material Managed by the FAA Depot
- Order AF 6000.10, Airway Facilities Service Maintenance Program
- Order 6000.54, Airway Facilities Hazard Communication Program
- Order 6000.15, General Maintenance Handbook for Airway Facilities
- Order 6000.30, National Airspace Maintenance Policy
- Order 6000.46, Maintenance Management System (MMS) Software Operations and Management
- Order 6000.48, General Maintenance Logging Handbook
- Order 6000.50, Airway Facilities National Airspace System Operations Handbook
- Order 6000.53, Remote Maintenance Monitoring Interfaces
- Order 6030.31, Restoration of Operational Facilities
- Order 6030.41, Notification Plan for Unscheduled Facility and Service Interruptions and Other Significant Events
- Order 6032.1, Modification to Ground Facilities, Systems, and Equipment in the National Airspace System
- Order 6040.6, Airway Facilities NAS Technical Evaluation Program
- Order 6040.15, NAS Performance Reporting System
- Order 6300.13, Radar Systems Optimization and Flight Inspection Handbook

- Order 7900.4, Reporting of Military-Certified Air Navigation Facilities to the NFDC (RIS: AT 7900-20)
- Order 7920.1, Content Criteria for Airman's Information Publications Originating in the NFDC

Flight Procedures:

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

New Systems:

- Order 4400.57, System for Acquisition Management
- The Federal Aviation Administration Acquisition Management System
- System Safety Management Program (SSMP)
- System Safety Handbook (SSH)
- System Engineering Manual (SEM)

Safety Risk Management:

- Order 8040.4, Safety Risk Management

Appendix B – Hazard Identification Tools

The descriptions in this appendix are designed to provide additional information regarding the hazards identification tools described in Table 4.1 (Section 4.37). In addition to the contents of this manual, more information concerning hazard identification and these tools can be found in the FAA's System Safety Handbook (<http://www.asy.faa.gov/Risk/SSHandbook/cover.htm>).

FUNCTIONAL HAZARD ANALYSIS

FORMAL NAME: Functional Hazard Analysis (FHA)

ALTERNATIVE NAMES: Functional Hazard Assessment

PURPOSE: To determine "what" a system or procedure must do in order to complete a mission or higher function. The failure or anomalous behavior of these functions is identified as a hazard and ranked according to severity based on its operational effect.

DESCRIPTION: An FHA is a systematic, comprehensive, and qualitative assessment of the basic known functions of a system. A function is a characteristic action or activity that has to be performed in order to achieve a desired system objective. It is "what" must be done and not "how." The primary basis for the FHA system description is a functional analysis in the form of functional flow diagrams, N2 charts and other tools used to describe the system's functionality (See FAA System Engineering Manual section 4.4). Since functions are hierarchical, that is functions are composed of sub-functions at multiple levels, an FHA is also done at multiple levels from the top-level system down to the system's constituent parts. A system level FHA, conducted at the beginning of the system development cycle, should identify and classify the hazards associated with the system level functions. The classification of severity of these hazards establishes the safety requirements that the system must meet. The goal of conducting an FHA is to clearly identify each functional hazard along with the rationale for its severity classification (i.e. catastrophic, hazardous, major, etc.) with the purpose of establishing the associated safety requirements for the system.

After system level functions have been used to derive system level requirements in the development process, each sub-system that represent the constitution of the system should be further examined at the next lower level of functions. In so doing, the FHA is an iterative process and becomes more defined and fixed as the system definition matures.

An FHA considers failure and/or anomalous behaviors that affect functions as hazards. Assessment of particular solutions, such as specific hardware or software, is not the goal of an FHA. Design Assurance of the system depends on the severity classification given to the functional hazards.

FAULT/FAILURE HAZARD ANALYSIS

FORMAL NAME: Fault/Failure Hazard Analysis

ALTERNATIVE NAMES: None

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

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

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

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

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

ALTERNATIVE NAMES: None

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

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

Hazard analyses consider failures, operating procedures, human factors, and transient conditions in the list of hazard causes. The FMECA is more limited. It only considers failures (hardware and software). It is generated from a different set of questions than the hazard analysis:

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

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

THE OPERATIONS ANALYSIS AND FLOW DIAGRAM

FORMAL NAME: The Operations Analysis (OA)

ALTERNATIVE NAMES: The flow diagram, flow chart, operation timeline

PURPOSE: To provide an itemized sequence of events or a flow diagram depicting the major events of an operation. This assures that all elements of the operation are evaluated as potential sources of risk. This analysis overcomes the weakness of only focusing on one or two aspects of an operation that are intuitively identified as risky, often to the exclusion of other aspects that may actually be riskier. The OA also guides the allocation of risk management resources over time as an operation unfolds event by event in a systematic manner.

APPLICATION: The OA or flow diagram is used in nearly all risk management applications, including the most time-critical situations. It responds to the key risk management question “What am I facing here and from where can risk arise?”

METHOD: Whenever possible, the OA is taken directly from the planning of the operation. It is difficult to plan an operation without listing the key events in a time sequence. If for some reason such a list is not available, the analyst creates one using the best available understanding of the operation. The best practice is to break down the operation into time-sequenced segments by tasks and activities. Normally, this is well above the detail of individual tasks. It may be appropriate to break down aspects of an operation that carry obviously higher risk into more detail than less risky areas. The product of an OA is a compilation of the major events of an operation in sequence, with or without time checks. Putting the steps of the process on index cards or sticky-back note paper allows the diagram to be rearranged without erasing and redrawing, thus encouraging contributions.

THE PRELIMINARY HAZARD ANALYSIS

FORMAL NAME: Preliminary Hazard Analysis (PHA)

ALTERNATIVE NAMES: The PHA

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

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

METHOD: The PHA is usually based on the Operations Analysis or flow diagram, taking each event in turn from it. Analysts apply their experience and intuition, use reference publications and standards of various kinds, and consult with personnel who may have useful input. The extent of the effort is dictated by resource and time limitations, and by the estimate of the degree of overall risk inherent in the operation. Hazards that are detected are often listed directly on a copy of the Operations Analysis. Alternatively, a more formal PHA format such as the worksheet, shown in the following example, can be used. The completed PHA is used to identify hazards requiring more in-depth hazard identification. Key to the effectiveness of the PHA is assuring that all events of the operation are addressed.

Ensure adequate space on the worksheet between each event to allow several hazards to be noted for each event. List the hazards noted for each operational phase. Strive for detail within the limits imposed by time. A copy of a PHA accomplished for an earlier similar operation would aid in the process.

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

EXAMPLE: The following is an example of a PHA.

MOVING A HEAVY PIECE OF EQUIPMENT

The example below uses an Operation Analysis for moving a heavy piece of equipment as the start point and illustrates the process of building the PHA directly from the Operations Analysis.

Operation: Move a 3-ton machine from one building to another.

Start Point: The machine is in its original position in building A

End Point: The machine is in its new position in building B

ACTIVITY/EVENT	HAZARD
Raise the machine to permit positioning of the forklift	<ul style="list-style-type: none"> • Machine overturns due to imbalance • Machine overturns due to failure of lifting device • Machine drops on person or equipment due to failure of lifting device or improper placement (person lifting device) • Machine strikes overhead obstacle • Machine is damaged by the lifting process
Position the forklift	<ul style="list-style-type: none"> • Forklift strikes the machine • Forklift strikes other items in the area
Lift the machine	<ul style="list-style-type: none"> • Machine strikes overhead obstacle • Lift fails due to mechanical failure (damage to machine, objects, or people) • Machine overturns due to imbalance
Move machine to the truck	<ul style="list-style-type: none"> • Instability due to rough surface or weather condition • Operator error causes load instability • The load shifts
Place machine on the truck	<ul style="list-style-type: none"> • Improper tie down produces instability • Truck overloaded or improper load distribution
Drive truck to building B	<ul style="list-style-type: none"> • Vehicle accident during the move • Poor driving technique produces instability • Instability due to road condition
Remove machine from the truck	<ul style="list-style-type: none"> • Same factors as “Move it to the truck”
Place machine in proper position in building B	<ul style="list-style-type: none"> • Same factors as “Raise the machine” except focused on lowering the machine

THE “WHAT IF” TOOL

FORMAL NAME: The “What If” Tool

ALTERNATIVE NAMES: None

PURPOSE: To identify hazards. The “What If” Tool is one of the most powerful hazard identification tools. As in the case of the Scenario Process Tool (see page B-9), it is designed to add structure to the intuitive and experiential expertise of operational personnel. The “What If” Tool is especially effective in capturing hazard data about failure modes that may create hazards. It is somewhat more structured than the Preliminary Hazard Analysis (PHA). Because of its ease of use, it is probably the single most practical and effective tool for use by operational personnel.

APPLICATION: The “What If” Tool should be used in most hazard identification applications, including many time-critical applications. A classic use of the “What If” Tool is as the first tool used after the Operations Analysis and the PHA. For example, the PHA reveals an area of hazard that needs additional investigation. The best single tool to further investigate that area will be the “What If” Tool. The user will zoom in on the particular area of concern, add detail to the OA in this area, and then use the “What If” procedure to identify the hazards.

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

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

The “What If” analysis can be expanded to further explore the hazards in an operation by developing short scenarios that reflect the worst credible outcome from the compound effects of multiple hazards in the operation. Follow these guidelines in writing scenarios:

- Target length is 5 or 6 sentences, 60 words
- Do not dwell on grammatical details
- Include elements of Mission, Man, Machine, Management, and Media
- Start with history
- Encourage imagination and intuition
- Carry the scenario to the worst credible outcome
- Use a single person or group to edit

EXAMPLE: Following is an extract from the typical output from the “What If” Tool.

Situation: Picture a group of 3 operational employees informally applying the round robin procedure for the “What If” Tool to a task to move a multi-ton machine from one location to another. A part of the discussion might go as follows:

Joe: What if the machine tips over and falls breaking the electrical wires that run within the walls behind it?

Bill: What if it strikes the welding manifolds located on the wall on the West Side? (*This illustrates “piggybacking” as Bill produces a variation of the hazard initially presented by Joe*).

Mary: What if the floor fails due to the concentration of weight on the base of the lifting device?

Joe: What if the point on the machine used to lift it is damaged by the lift?

Bill: What if there are electrical, air pressure hoses, or other attachments to the machine that are not properly neutralized?

Mary: What if the lock out/tag out is not properly applied to energy sources servicing the machine? And so on....

Note: The list above might be broken down as follows:

Group 1: Machine falling hazards

Group 2: Weight induced failures

Group 3: Machine disconnect and preparation hazards

These related groups of hazards are then subjected to the remaining five steps of the operational risk management (ORM) process.

THE SCENARIO PROCESS TOOL

FORMAL NAME: The Scenario Process Tool

ALTERNATIVE NAMES: The Mental Movie Tool.

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

APPLICATION: The Scenario Process Tool should be used in most hazard identification applications, including some time-critical applications. In the time-critical mode, it is indeed one of the few practical tools, in that the user can quickly form a “mental movie” of the flow of events immediately ahead and the associated hazards.

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

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

EXAMPLE: Following is an example of the Scenario Process Tool; Machine Movement Scenario.

FROM MACHINE MOVEMENT EXAMPLE: As the machine was being jacked-up to permit placement of the forklift, the fitting that was the lift point on the machine broke. The machine tilted in that direction and fell over striking the nearby wall. This in turn, broke a fuel gas line in the wall. The gas was turned off as a precaution, but the blow to the metal line caused the valve to which it was attached to break, releasing gas into the atmosphere. The gas quickly reached the motor of a nearby fan (not explosion proof) and a small explosion followed. Several personnel were badly burned and that entire section of the shop was badly damaged. The shop was out of action for 3 weeks.

THE LOGIC DIAGRAM

FORMAL NAME: The Logic Diagram

ALTERNATIVE NAMES: The Logic Tree

PURPOSE: To provide structure and detail as a primary hazard identification procedure. Its graphic structure is an excellent means of capturing and correlating the hazard data produced by other primary tools. Because of its graphic display, it can also be an effective hazard-briefing tool. The more structured and logical nature of the Logic Diagram adds substantial depth to the hazard identification process to complement the other more intuitive and experiential tools. Finally, the Logic Diagram establishes the connectivity and linkages that often exist between hazards. It does this very effectively through its tree-like structure.

APPLICATION: Because it is more structured, the Logic Diagram requires considerable time and effort to accomplish. Following the principles of SRM, its use will be more limited than the other primary tools. This means limiting its use to higher risk issues. By its nature, it is most effective with more complicated operations in which several hazards may be interlinked. Because it is more complicated than the other primary tools, it requires more practice, and may not appeal to all operational personnel. However, in an organizational climate committed to SRM excellence, the Logic Diagram will be a welcomed and often used addition to the hazard identification toolbox.

METHOD: There are three types of Logic Diagrams. These are the:

Positive diagram. This variation is designed to highlight the factors that must be in place if risk is to be effectively controlled in the operation. It works from a safe outcome back to the existing factors that produce it.

Event diagram. This variation focuses on an individual operational event (often a failure or hazard identified using the “What If” tool) and examines the possible consequences of the event. It works from an event that may produce risk and shows what the loss outcomes of the event may be.

Negative diagram. This variation selects a loss event and then analyzes the various hazards that could combine to produce that loss. It works from an actual or possible loss and identifies what factors could produce it.

All of the various Logic Diagram options can be applied either to an actual or planned operating system. Of course, the best time for application is in the planning stages of the operational lifecycle. All of the Logic Diagram options begin with a top block. In the case of the positive diagram, this is a desired outcome; in the case of the event diagram, this is an operations event or contingency possibility; in the case of the negative diagram, it is a loss event. When working with positive diagram or negative diagram, the user then, reasons out the factors that could produce the top event. These are entered on the next line of blocks. With the event diagram, the user lists the possible results of the event being analyzed. The conditions that could produce the

factors on the second line are then considered and they are entered on the third line. The goal is to be as logical as possible when constructing Logic Diagrams, but it is more important to keep the hazard identification goal in mind than to construct a masterpiece of logical thinking. Therefore, a Logic Diagram should be a worksheet with many changes and variations. With the addition of a chalkboard or flip chart, it becomes an excellent group tool.

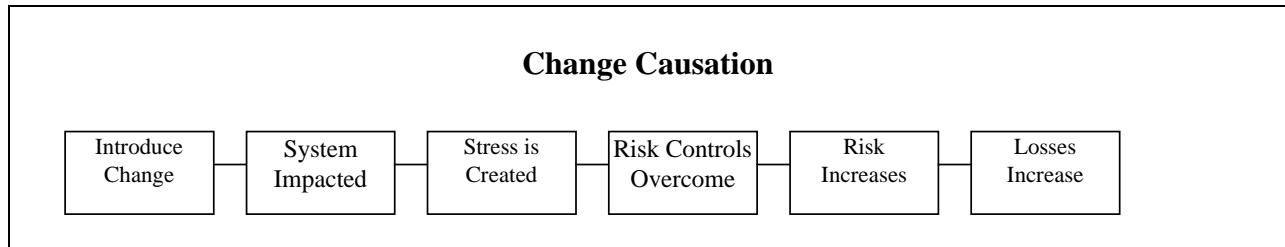
THE CHANGE ANALYSIS

FORMAL NAME: The Change Analysis

ALTERNATIVE NAMES: None

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

The following figure illustrates this causal relationship.



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

APPLICATION: Change analysis should be routinely used in the following situations.

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

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

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

Sample Change Analysis Worksheet

Target: _____ Date: _____				
FACTORS	EVALUATED SITUATION	COMPARABLE SITUATION	DIFFERENCE	SIGNIFICANCE
WHAT Objects Energy Defects Protective Devices				
WHERE On the object In the process Place				
WHEN In time In the process				
WHO Operator Fellow worker Supervisor Others				
TASK Goal Procedure Quality				
WORKING CONDITIONS Environmental Overtime Schedule Delays				
TRIGGER EVENT MANAGERIAL CONTROLS Control Chain Hazard Analysis Monitoring Risk Review				
To use the worksheet: The user starts at the top of the column and considers the current situation compared to a previous situation and identifies any change in any of the factors. When used in an accident investigation, the accident situation is compared to a previous baseline. The significance of detected changes can be evaluated intuitively or they can be subjected to "What If," Logic Diagram, or scenario, other specialized analyses.				

THE CAUSE AND EFFECT TOOL

FORMAL NAME: The Cause and Effect Tool

ALTERNATIVE NAMES: The Cause and Effect Diagram. The Fishbone Tool, the Ishikawa Diagram

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

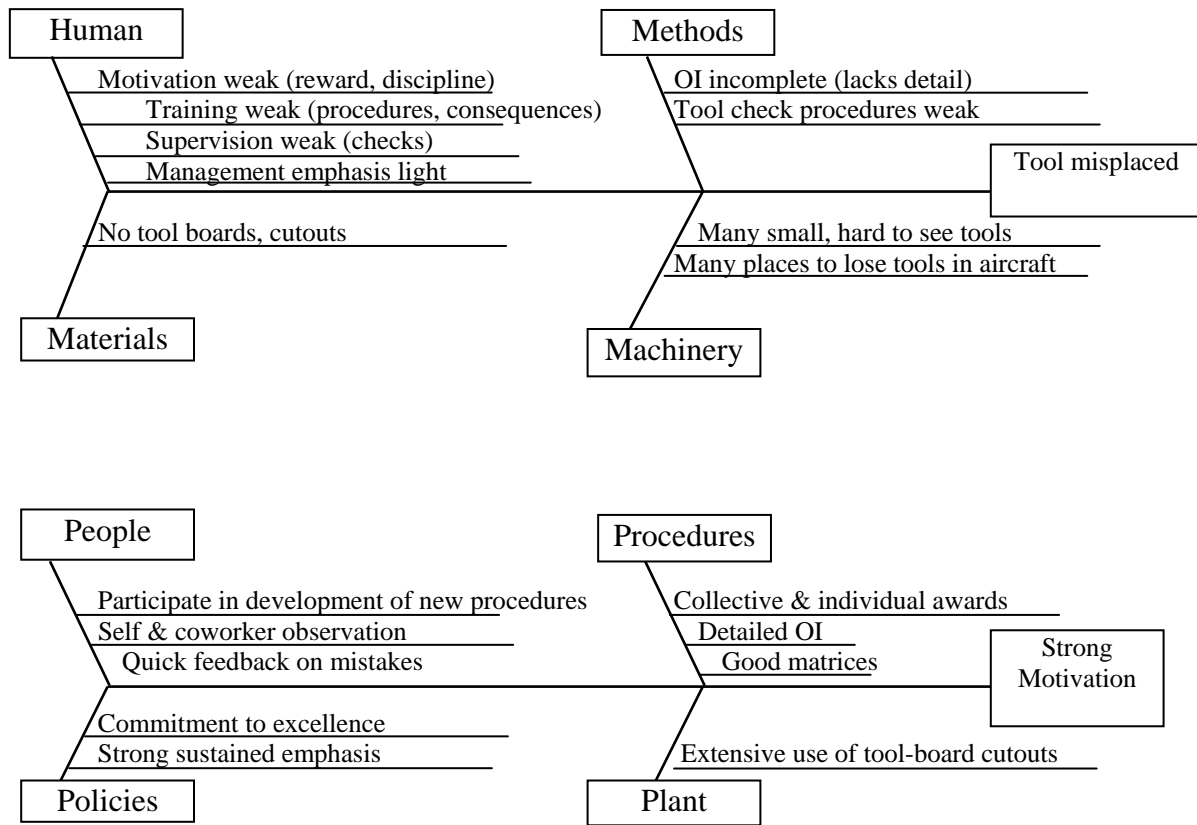
APPLICATION: The Cause and Effect Tool will be effective in organizations that have had some success with the quality initiative. It should be used in the same manner as the Logic Diagram and can be applied in both a positive and negative variation.

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

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

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

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



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

THE HAZARD AND OPERABILITY TOOL

FORMAL NAME: The Hazard and Operability Tool (HAZOP)

ALTERNATIVE NAMES: The HAZOP Analysis

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

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

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

Standard HAZOP Guidewords:

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

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

THE MAPPING TOOL

FORMAL NAME: The Mapping Tool

ALTERNATIVE NAMES: Map Analysis

PURPOSE: To use terrain maps and other system models and schematics to identify both things at risk and the sources of hazards. Properly applied the tool will reveal the following:

- Task elements at risk
- The sources of risk
- The extent of the risk (proximity)
- Potential barriers between hazard sources and operational assets

APPLICATION: The Mapping Tool can be used in a variety of situations. The explosive quantity-distance criteria are a classic example of map analysis. The location of the flammable storage is plotted and then the distance to various vulnerable locations (inhabited buildings, highways, etc.) is determined. The same principles can be extended to any facility. We can use a diagram of a maintenance shop to note the location of hazards such as gases, pressure vessels, flammables, etc. Key assets can also be plotted, hazardous interactions are noted and the layout of the facility can be optimized in terms of risk reduction.

METHOD: The Mapping Tool requires some creativity to realize its full potential. The starting point is a map, facility layout, or equipment schematic. The locations of hazard sources are noted. The easiest way to detect these sources is to locate energy sources since all hazards involve the unwanted release of energy. The following table lists the types of energy to look for. Mark the locations of these sources on the map or diagram. Then, keeping the operation in mind, locate the personnel, equipment, and facilities that the various potentially hazardous energy sources could impact. Note these potentially hazardous links and enter them in the hazard inventory for risk management purposes.

Major Types of Energy:

- Electrical
- Kinetic (moving mass, e.g., a vehicle, a machine part, a bullet)
- Potential (not moving mass, e.g., a heavy object suspended overhead)
- Chemical (e.g., explosives, corrosive materials)
- Noise and Vibration
- Thermal (heat)
- Radiation (Non-ionizing, e.g., microwave, and ionizing, e.g., nuclear radiation, x-rays)
- Pressure (air, hydraulic, water)

THE INTERFACE ANALYSIS

FORMAL NAME: The Interface Analysis

ALTERNATIVE NAMES: Interface Hazard Analysis

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

APPLICATION: An Interface Analysis should be conducted any time a new activity is being introduced and there is any chance at all that unfavorable interaction could occur. A good cue to the need for an Interface Analysis is the use of either the Change Analysis (indicating the injection of something new) or the map analysis (with the possibility of interactions).

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

The Interface Analysis Worksheet

Energy Element:

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

Personnel Element: Personnel moving from one area to another

Equipment Element: Machines and material moving from one area to another

Supply/materiel Element:

- Intentional movement from one area to another
- Unintentional movement from one area to another

Product Element: Movement of product from one area to another

Information Element: Flow of information from one area to another or interference (i.e., jamming)

Bio-material Element:

- Infectious materials (virus, bacteria, etc.)
- Wildlife
- Odors

THE ACCIDENT / INCIDENT ANALYSIS

FORMAL NAME: The Accident/Incident Analysis

ALTERNATIVE NAMES: The Accident Analysis

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

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

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

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

THE INTERVIEW TOOL

FORMAL NAME: The Interview Tool

ALTERNATIVE NAMES: None

PURPOSE: To capture the experience of personnel in ways that are efficient and positive for them. Often the most knowledgeable personnel in the area of risk are those who operate the system. They see the problems and often think about potential solutions. Properly implemented, the Interview Tool can be among the most valuable hazard identification tools.

APPLICATION: Every organization can use the Interview Tool in one form or another.

METHOD: The Interview Tool's great strength is versatility. The figure below illustrates the many options available to collect interview data. Key to all of these is to create a situation in which interviewees feel free to honestly report what they know, without fear of any adverse consequences. This means absolute confidentiality or anonymity must be assured.

Interview Tool Alternatives:

- Direct interviews with operational personnel
- Supervisors interview their subordinates and report results
- Questionnaire interviews are completed and returns
- Group interview sessions (several personnel at one time)
- Hazards reported formally
- Coworkers interview each other

THE INSPECTION TOOL

FORMAL NAME: The Inspection Tool

ALTERNATIVE NAMES: The Survey Tool

PURPOSE: Inspections have two primary purposes: (1) The detection of hazards. Inspections accomplish this through the direct observation of operations. The process is aided by the existence of detailed standards against which operations can be compared. The OSHA standards and various national standards organizations provide good examples. (2) To evaluate the degree of compliance with established risk controls. When inspections are targeted at management and safety management processes, they are usually called surveys. These surveys assess the effectiveness of management procedures by evaluating status against some survey criteria or standard. Inspections are also important as accountability tools and can become training opportunities

APPLICATION: Inspections and surveys are used in the risk management process in much the same manner as in traditional safety programs. Where the traditional approach may require that all facilities are inspected on the same frequency schedule, the SRM concept might dictate that high-risk activities be inspected ten times or more frequently than lower risk operations, and that some of the lowest risk operations be inspected once every five years or so. The degree of risk drives the frequency and depth of inspections and surveys.

METHOD: There are many methods of conducting inspections. From a risk management point of view, the key is focusing upon what will be inspected. The first step in effective inspections is the selection of inspection criteria and the development of a checklist or protocol. This must be risk-based. Commercial protocols are available that contain criteria validated to be connected with safety excellence. Alternatively, excellent criteria can be developed using incident databases and the results of other hazard identification tools such as the Operations Analysis. Some these have been computerized to facilitate entry and processing of data. Once criteria are developed, a schedule is created and inspections begin. The inspection itself must be as positive an experience as possible for the people whose activity is being inspected. Personnel performing inspections should be carefully trained, not only in the technical processes involved, but also in human relations. During inspections, the SRM concept encourages another departure from traditional inspection practices. This makes it possible to evaluate the trend in organization performance by calculating the percentage of unsafe (non-standard) versus safe (meet or exceed standard) observations. Once the observations are recorded, the data must be carefully entered in the overall hazard inventory database. Once in the database, the data can be analyzed as part of the overall body of data or as a mini-database composed of inspection findings only.

THE JOB HAZARD ANALYSIS

FORMAL NAME: The Job Hazard Analysis (JHA)

ALTERNATIVE NAMES: The Task Hazard Analysis, Job Safety Analysis, THA, JSA

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

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

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

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

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

THE OPPORTUNITY ASSESSMENT

FORMAL NAME: The Opportunity Assessment

ALTERNATIVE NAMES: The Opportunity-Risk Tool

PURPOSE: To identify opportunities to expand the capabilities of the organization and/or to significantly reduce the operational cost of risk control procedures.

APPLICATION: Organizations should systematically assess their capabilities on a regular basis, especially in critical areas. The Opportunity Assessment can be one of the most useful tools in this process, and thus should be completed on all critical operations and periodically updated.

METHOD: The Opportunity Assessment involves five key steps as outlined below. Step 1, identifies and prioritizes operational areas that would benefit substantially from expanded capabilities. Additionally, areas where risk controls are consuming extensive resources or are otherwise constraining operation capabilities are listed and prioritized. Step 2 involves the analysis of the specific risk-related barriers that are limiting the desired expanded performance or causing the significant expense- this is a critical step. Only by identifying the risk issues precisely can focused effort be brought to bear to overcome them. Step 3 attacks the barriers by using the safety risk management (SRM) process. This normally requires reassessment of the hazards, application of improved risk controls, improved implementation of existing controls, or a combination of these options. Step 4 is when available SRM procedures do not appear to offer any breakthrough possibilities. In these cases, the organization must seek out new SRM tools using benchmarking procedures or, if necessary, innovate new procedures. Step 5 requires the exploitation of any breakthroughs achieved by pushing the operational limits or cost saving until a new barrier is reached. The cycle then repeats and a process of continuous improvement begins.

Opportunity Analysis Steps:

- Step 1. Review key operations to identify opportunities for enhancement - prioritize
- Step 2. In areas where opportunities exist, analyze for risk barriers
- Step 3. When barriers are found, apply the SRM process
- Step 4. When available SRM processes can't breakthrough, innovate!
- Step 5. When a barrier is breached, push through until a new barrier is reached

THE ENERGY TRACE AND BARRIER ANALYSIS

FORMAL NAME: The Energy Trace and Barrier Analysis (ETBA)

ALTERNATIVE NAMES: Abnormal Energy Exchange

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

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

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

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

Types of Energy:

- Electrical
- Kinetic (moving mass, e.g., a vehicle, a machine part, a bullet)
- Potential (not moving mass, e.g., a heavy object suspended overhead)
- Chemical (e.g., explosives, corrosive materials)
- Noise and Vibration
- Thermal (heat)
- Radiation (Non-ionizing, e.g., microwave, and ionizing, e.g., nuclear radiation, x-rays)
- Pressure (air, hydraulic, water)

THE FAULT TREE ANALYSIS

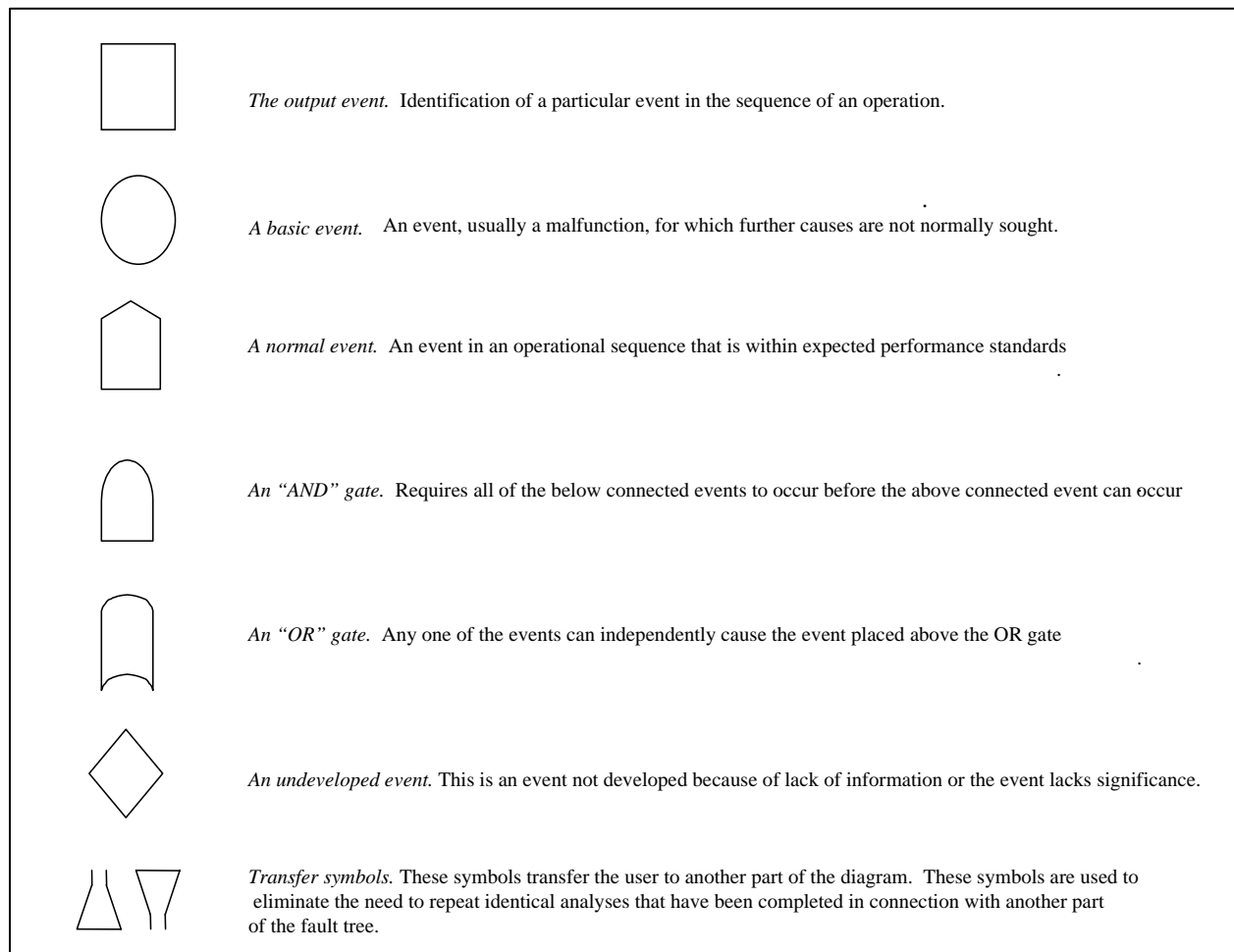
FORMAL NAME: The Fault Tree Analysis (FTA)

ALTERNATIVE NAMES: The Logic Tree

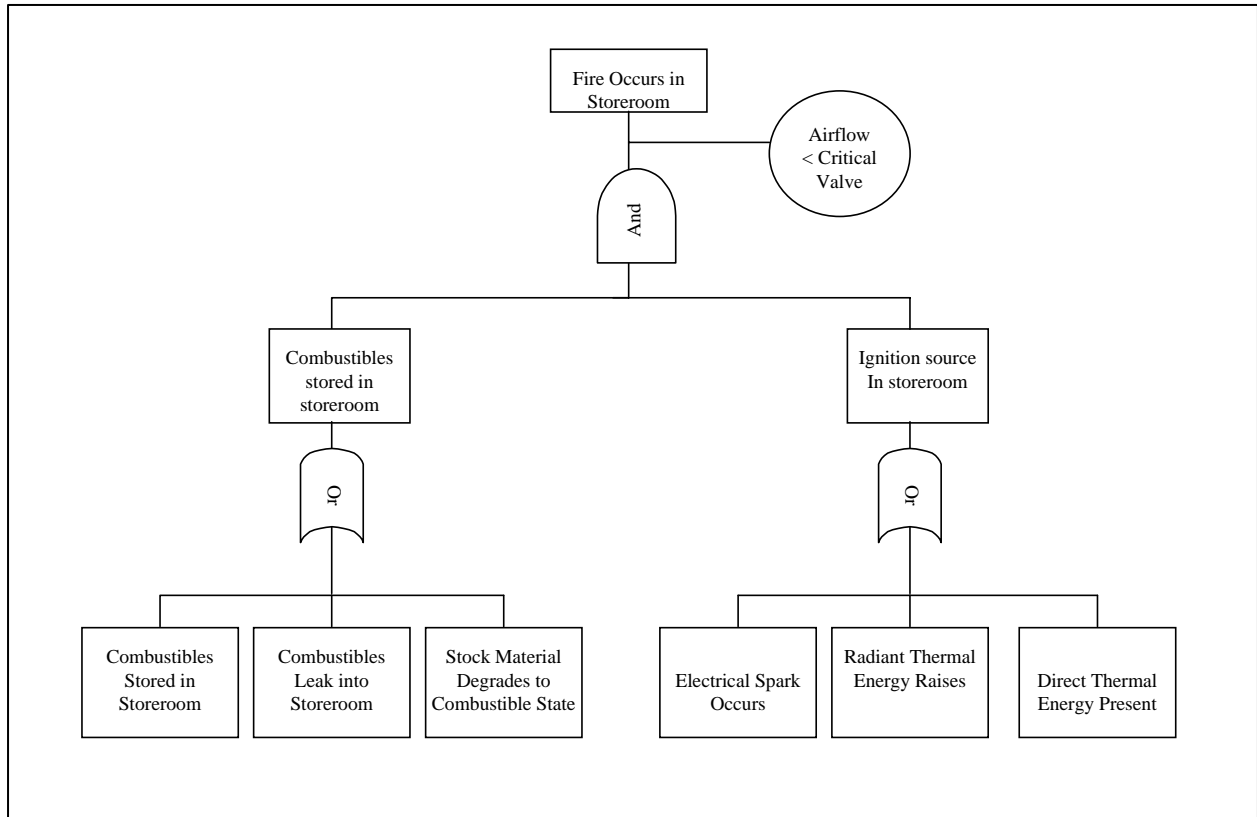
PURPOSE: To add hazard identification value to the basic Logic Diagram. The Fault Tree Analysis (FTA) is a hazard identification tool based on the negative type Logic Diagram. The FTA adds several dimensions to the basic logic tree. The most important of these additions are the use of symbols to add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

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

METHOD: The FTA is constructed using the following symbols:



EXAMPLE: A brief example of the FTA illustrates how an event may be traced to specific causes that can be very precisely identified at the lowest levels. See below for an example of FTA.



THE MULTI-LINEAR EVENTS SEQUENCING TOOL

FORMAL NAME: The Multi-linear Events Sequencing Tool (MES)

ALTERNATIVE NAMES: The Timeline Tool, the Sequential Time Event Plot (STEP)¹⁶

PURPOSE: To detect hazards arising from the time relationship of various operational activities. The MES detects situations in which either the absolute or relative timing of events may create risk. For example, an operational planner may have crammed too many events into a single period of time, creating a task overload problem for the personnel involved. Alternatively, the MES may reveal that two or more events in an operational plan conflict because a person or piece of equipment is required for both, but obviously cannot be in two places at once. The MES can be used as a hazard identification tool or as an incident/accident investigation tool.

APPLICATION: The MES is usually considered a loss prevention method, but the MES worksheet simplifies the process to the point that a motivated individual can effectively use it. The MES should be used any time that risk levels are significant and when timing and/or time relationships may be a source of risk. It is an essential tool when the time relationships are relatively complex.

METHOD: The MES uses a worksheet similar to the one illustrated below. The sample worksheet displays the timeline of the operation across the top and the “actors” (people or things) down the left side. The flow of events is displayed on the worksheet, depicting the relationship between the actors on a time basis. Once the operation is displayed on the worksheet, the sources of risk will be evident as the flow is examined.

Multi-linear Events Sequencing Form:

Timeline	(Time units in seconds or minutes as needed)
Actors	
(People or things involved in the process)	

¹⁶ K. Hendrisk, and L. Benner, *Investigating Accidents with Step*, Marcel Dekker, New York, 1988.

THE MANAGEMENT OVERSIGHT AND RISK TREE

FORMAL NAME: The Management Oversight and Risk Tree (MORT)

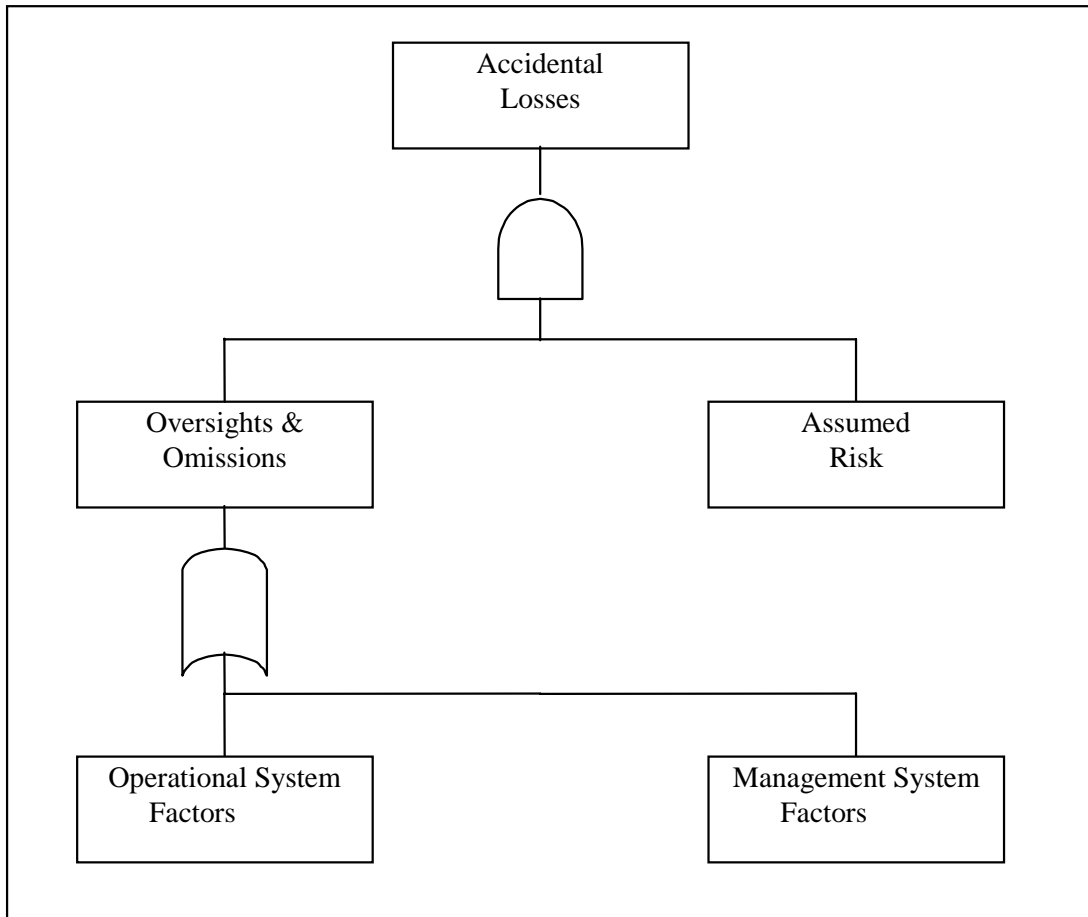
ALTERNATIVE NAMES: The MORT

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

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

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

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



FAA OPERATIONAL SUPPORT TEST AND EVALUATION (T&E) GOLD STANDARD PROCESS

FORMAL NAME: T&E Gold Standard Process

ALTERNATIVE NAMES: None

PURPOSE: To develop, test and deliver new hardware and software modifications to the field. The T&E Gold Standard Process for hardware and software modifications consists of four primary attributes. Specifically:

1. A standardized six-step process to be implemented by all programs. This process includes specific exit criteria that document the status of the completed development and T&E activities.
2. The identification and use of automated test tools and realistic test environments to maximize T&E prior to operational use.
3. Improved communication with the field regarding the development and T&E milestones completed via the delivery of the T&E Entrance and Exit Criteria Summary. This will provide a clear indication of processes followed and any limitations that occurred.
4. The identification of each organization or group's involvement in the T&E process.

APPLICATION: The T&E Gold Standard Process is comprised of six general phases conducted to develop, test, and deliver new hardware and software modifications to the field. They are:

- Needs and Requirements (Define It)
- Design and Development (Design It)
- Development Test (Build It)
- System Test (Test It)
- Key Site Test (Deploy It)
- Field Acceptance Test and Familiarization (Deliver It)

METHOD: In each of these six phases, specific entrance and exit criteria have been identified. Proceeding from one phase to the next is dependent on the successful completion of these criteria. During the Needs & Requirements and Design & Development phases, requirements are clearly defined and prioritized for release by the stakeholder/user. Preliminary Design Review (PDR) and Critical Design Review (CDR) activities are conducted and a development peer review process (as required for FAA ...Integrated Capability Maturity Model ® (FAA-iCMM ®) Level 3 certification) is practiced.

Development Test begins after the first two phases are successfully completed and ensure that new functionality works properly and interrelated functions are not adversely affected. During this phase, a system test plan is completed.

The fourth phase, System Test, is one of the most critical in ensuring that existing system functionality or baseline performance is revalidated and new functionality or fixes are verified,

including a documented procedure to regress back to the existing hardware and software baseline. The team that performs this test should be independent of the development test activities.

Following successful completion of System Test, Key Site Testing is performed to validate performance in a more realistic operational environment. The Key Site is chosen to verify any functions that could not be verified during System Test and is conducted with the system fully site adapted. Based on the results of Key Site Test, the national delivery package is finalized.

The final step of the process, Field Acceptance Test and Familiarization, is conducted at all downstream sites and is done to validate performance prior to operational use.

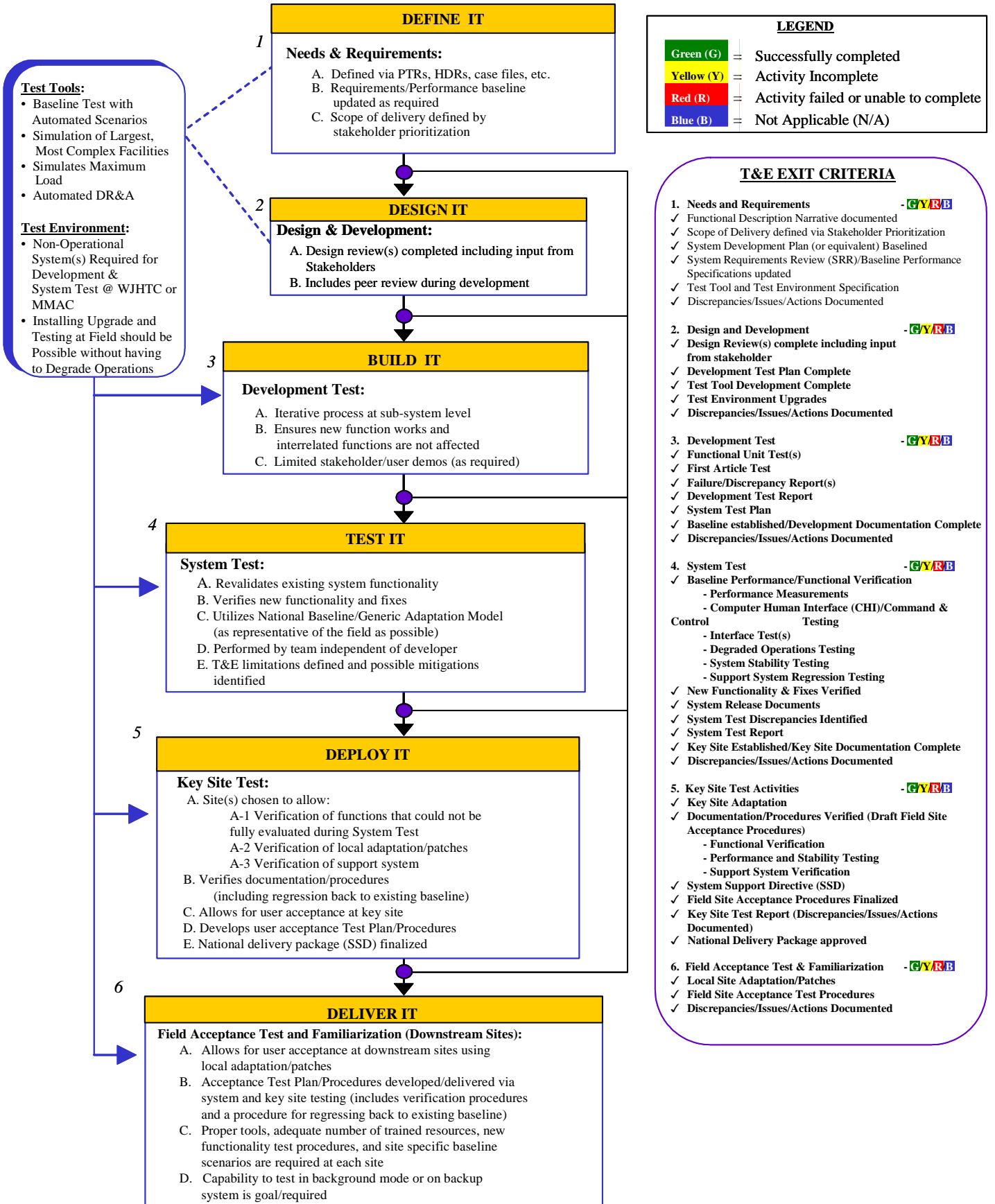
Test Tools and Test Environment: To perform both a timely and thorough validation of system performance and functionality using the six phase T&E Gold Standard Process, adequate Test Tools are required. These Test Tools provide:

- an automated Data Recording and Analysis (DR&A) capability
- an automated baseline scenario test that can simulate maximum loading on the system and also closely replicates the loading found at the largest most complex facility
- an automated scenario generation capability for all new systems

The Test Environment available at both the non-operational and operational facilities should allow maximum verification prior to operational use. In the non-operational environment (e.g., support systems at the FAA Technical Center or Logistics Center), the systems should be configured as similarly as possible to the fielded baseline and should verify all external interfaces. In the operational environment, back-up, redundant channel, or system capability should be used when available.

Better Communication: To ensure that a structured T&E process has been followed, a key attribute of the proposed Gold Standard Process is the concept of both defining and adhering to exit criteria. To improve the communications with the field, a T&E Entrance and Exit Criteria Summary with color indicators of success (green, yellow, and red) will accompany a hardware and software system delivery. This summary will be used to clearly communicate to FAA field personnel the T&E activities that have been completed as well as to identify any limitations (e.g., the fact that a particular interface could not be tested). In addition, the summary will clearly indicate where steps were not completed either because they were not deemed to be required, schedule pressure, or external pressures to deliver the modification prevented completion.

The following is a diagram of the T&E Gold Standard Process for delivery of hardware and software modifications, Version 1.0, December 10, 2001:



Appendix C – SRM and Changes to Air Traffic Control Procedures

C.1 *How do I apply SRM to changes to ATC procedures?*

As was discussed Chapter 4, *Safety Risk Management Guidance*, the SMS and its procedures apply to air traffic operations, maintenance, airspace and procedures development, airports, new systems, and modifications to existing systems (hardware and software).

ATC procedures, in most cases, have safety implications and can involve various equipment and systems to execute tasks associated with ATC. Each of these procedures and changes to these procedures must be safe, and compatible with others they affect.

The fundamental process for assessing the risk associated with ATC procedures is the same as for any other change. The five-phase process discussed in Chapter 4, *Safety Risk Management Guidance*, needs to be followed. This section offers additional guidance related specifically to the assessment of ATC procedures.

C.2 *What expertise do SRM Panels require?*

Though a single specialist and practitioner can assess some procedural changes, in general safety risk assessment of ATC procedures is best conducted by an SRM Panel, as described in Chapter 4, (Sections 4.55 – 4.57). Though the make-up of the Panel will vary with the complexity of the procedure and change, consideration should be given to including the following expertise on the SRM Panel:

- staff directly responsible for procedure design
- staff with current knowledge and experience of the procedural area under assessment (i.e., system users)
- engineering or automation expert - to provide knowledge on equipment performance
- safety management specialist - to guide the application of the methodology
- human factors specialist
- software specialist

C.3 *What are the steps used to assess an ATC procedural change?*

Risk assessment of ATC procedures involves the following steps:

Step 1. Identify whether the change involves a control procedure, change in equipment, or both.

Step 2. Breakdown the procedures into manageable components. For example, control procedures might be divided into:

- transfer of control procedures
- coordination procedures

- radar procedures
- holding procedures
- speed control procedures
- runway procedures

Equipment procedures might be divided into:

- set-up procedures
- operations under normal and emergency conditions
- operations under equipment failure or partial failure conditions

Step 3. Identify potential hazards that affect the ability to maintain safe separation. This is best achieved by the group asking “What can go wrong?” and “What if...?” in relation to the identified divisions in Step 2. Other tools that may be appropriate for use in assessing ATC procedures are: The Operations Analysis Tool, and the Scenario Process Tool. (Information on these and other hazard identification tools can be found on Appendix B.)

Step 4. The group assesses the hazard severity as described in Table 4.2 (Section 4.39).

Step 5. The group identifies the circumstances or incident sequence under which a hazard might occur and the likelihood of occurrence, as described in Table 4.3 (Section 4.40).

Step 6. The group examines the hazard and incident analysis and identifies risk mitigation measures where necessary. More information on risk mitigation can be found in Sections 4.41 through 4.54.

Step 7. An SRMD is generated and approved as described in Chapter 5, *Safety Risk Management Documentation: Development and Approval*.

Appendix D – Documenting Safety Risk Management

A Safety Risk Management Document (SRMD) is a report that thoroughly describes the SRM process and documents evidence that a proposed change to a system is acceptably safe. Any change that could have safety consequences in the provision of air traffic service is documented.

At minimum, an SRMD must answer:

- What is the change?
- How has the safety risk of the change been assessed?
- What risk has been identified?
- How will the risks be mitigated and monitored?

Currently, many FAA organizations conduct and document safety risk management, however the types of processes utilized (analysis, testing, etc.) and the report formats may vary among organizations. Some of the components of an SRMD may be fulfilled through the inclusion of documentation produced through current safety risk management processes.

The list in the shaded box below describes the minimum contents of an SRMD.

SRMD Contents
<ul style="list-style-type: none">• description of the potential system state(s) – including the identification of any important support systems and interfaces without which the system could not achieve its functions• description of the proposed change• identified hazards (and description of hazard identification methodology)• estimation of risk• description of existing and planned mitigation• description of methodology for tracking hazards and verifying effectiveness of mitigation controls throughout the lifecycle of the system or change• method for monitoring of operational data to ensure hazards are controlled• identification of the organization responsible for the conduct of the analysis and tracking of the resolution, if any• current disposition of hazard mitigations• plan to verify that safety critical performance requirements are met• a recommendation concerning the implementation decision

For further guidance, a general template is provided on the following page.

The ATO Safety Service Unit plays an important role in ensuring the quality of SRMDs through consulting with SRM practitioners, auditing processes, and reviewing SRMDs.

Examples of actual SRMDs will be included in future versions of this manual.

GENERAL INSTRUCTIONS FOR COMPLETING THE SAFETY RISK MANAGEMENT DOCUMENT (SRMD)

A Safety Risk Management Document (SRMD) is a report that thoroughly describes the SRM process for a proposed change to the National Airspace System (NAS) and documents the associated risk is acceptable. The SRMD provides the findings in a clear, concise manner that decision-makers can understand and use.

The template lists the eight major topics included in an SRMD. The scope and detail of the document will depend upon the magnitude and nature of the change.

Instructions:

- A. Complete the SRMD Template to help create a clear, readable, and concise presentation of the results of the safety risk assessment of a proposed change to the NAS.
- B. Address each of the components in the template.
- C. Collect the approving signatures, once the SRMD is completed.

1.0 Implementation Decision

The process for approval of the SRMD is dependent on the span of the program and the risk associated with the change. In general, the management official(s) who approves the SRMD certifies that the documentation was developed properly, hazards are systematically identified, and risk is appropriately estimated and mitigated. The approval signifies that the risk associated with the change is acceptable.

- a. Title:
- b. Originator:
- d. Originator's Organization:
- d. Originator's Phone Number:
- e. Sponsoring Organization:
- f. Sponsor's Focal Point:
- g. Sponsor's Focal Point Phone Number:
- h. Submission Date:
- i. SRMD Revision Number:
- j. SRMD Revision Date:

Approval Signature(s): (The level at which the approval is given correlates to the level of identified risk, and the span of the program and mitigation strategies.)

Appropriate Authority

Date

- 2.0 Current System (System Baseline)
Describe the current system and potential system state(s) – including the identification of any critical support systems and interfaces without which the system could not achieve its functions.
- 3.0 Proposed Change
Describe the proposed change to the NAS. When critical safety parameters are involved, identify the method that will be used to verify performance.
- 4.0 Identified Hazards
Describe the hazards identified. Include a description of the hazard identification methodology and tools utilized.
- 5.0 Estimated Risk
Estimate the risk of the change. Describe the methodology and tools utilized.
- 6.0 Hazard Mitigation and Tracking
Describe the hazard mitigation strategy and control efforts. Describe the methodology for tracking hazards and verifying effectiveness of mitigation controls throughout the lifecycle of the system or change. (Note: Hazard tracking is an essential element of SRM, which can be accomplished through the use of an automated system, as described in Chapter 4, Section 4.54).
- 7.0 Hazard Monitoring
Describe the method(s) that will be utilized for monitoring operational data to ensure hazards are controlled. (Note: The hazard tracking system must be linked to operational metrics to verify that the risk mitigation strategies are effective in controlling the hazard.)
- 8.0 Impacted Organizations
Identify the organizations that are impacted by the change and describe the method used for collaboration during the identification, mitigation, tracking, and monitoring of hazards.

Appendix E – Glossary of Terms

(These definitions are consistent with those included in the FAA AMS System Safety Management Plan, FAA System Safety Handbook, FAA Advisory Circular AC25.1309, and other FAA documents.)

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

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

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

Change. To modify, alter, or make different.

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

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

- (1) **Validated.** Validated controls are those controls and requirements that are unambiguous, correct, complete, and verifiable.
- (2) **Recommended.** Recommended controls are those controls that have the potential to mitigate a hazard or risk but have not yet been validated as part of the system or its requirements.
- (3) **Verified.** Verified controls are those controls and requirements that have met the implemented solution.

Design diversity. Independent generation of different implementations of the same logic function.

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

Equipment. Equipment is a complete assembly, operating either independently or within a subsystem or system, that performs a specific function.

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, subsystems, and equipment.

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

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

Process. An organized group of related activities that work together to produce a desirable condition.

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

Risk. Risk is the composite of predicted severity and likelihood of the potential effect of a hazard in the worst credible system state. There are three types of risk: (1) initial, (2) current, and (3) residual.

- (1) **Initial.** Initial risk is the severity and likelihood of a hazard when it is first identified and assessed. It is used to describe the severity and likelihood of a hazard in the beginning or very preliminary stages of a decision, program, or analysis. Initial risk is determined by factoring both verified controls and assumptions into the system state. When assumptions are made, they must be documented as recommended controls. Once the initial risk is established, it is not changed.
- (2) **Current.** Current risk is the predicted severity and likelihood of a hazard at the current time. When determining current risk, both validated controls and verified controls are factored into the risk assessment. Current risk may change based on the actions taken by the decision-maker that relate to the validation and/or verification of the controls associated with a hazard.
- (3) **Residual.** Residual risk is the remaining risk that exists after all control techniques have been implemented or exhausted, and all controls have been verified. Only verified controls can be used on the assessment of residual risk.

Safety requirement. A control written in requirements language.

Safety Management System (SMS). An integrated collection of processes, procedures, and programs that ensure a formalized and proactive approach to system safety through risk management. Risk assessments are required for all changes in order to identify safety impacts. The SMS is closed-loop, ensuring that all changes are documented and all problems or issues are tracked to conclusion.

Safety significant change. A change that impacts NAS safety and requires SRM as described in Figure 3.1 - *SRM Decision Process*.

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

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

System state. System state is an expression of the various conditions, characterized by quantities or qualities in which a system can exist.

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

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

Appendix F – Acronyms/Abbreviations

A/C - Aircraft

AAI - Office of Accident Investigation

AFS - Flight Standards Service

AIDS - Accident/Incident Reporting Data System

AMA - Mike Monroney Aeronautical Center - FAA Academy

AMS - Acquisition Management System

AOV - Air Traffic Safety Oversight Service

ARP - Airports Office

ASAP - Aviation Safety Action Program

ASRP - Aviation Safety Reporting Program

ASRS - Aviation Safety Reporting System

ASY - Office of System Safety

ATC - Air Traffic Control

ATM - Air Traffic Management

ATO - Air Traffic Organization

AVR - Office of Regulation and Certification

C-ARTS - Common Automated Radar Terminal System

CAA - Civil Aviation Authority

CBI - Computer-based Instruction

CDR - Critical Design Review

CFR - Code of Federal Regulations

CNS - Communications, Navigation, Surveillance

CONOPS - Concept of Operations

COO - Chief Operating Officer

CSA - Comparative Safety Assessment

DCP - Document Change Proposal

DP - Departure Procedures

DR&A - Data Reduction and Analysis

ETBA - Energy Trace-Barrier Analysis

ERAM - En Route Automation Modernization

ETMS - Enhanced Traffic Management System

FAA - Federal Aviation Administration
FAST - FAA Acquisition System Toolset
FHA - Functional Hazard Analysis
FMEA - Failure Modes and Effects Analysis
FMECA - Failure Modes, Effects, and Criticality Analysis
FMS - Flight Management System
FRDF - Facility Reference Data File
FSDO - Flight Standards District Office
FTA - Fault Tree Analysis
GAIN - Global Aviation Information Network
GAO - General Accounting Office
GPS - Global Positioning System
HAZOP - Hazard and Operability Tool
HMI - Human Machine Interface
HTTR - Hazard Tracking and Risk Resolution
HTS - Hazard Tracking System
H_z - Hazard
IAPA - Instrument Approach Procedures Automation
ICAO - International Civil Aviation Organization
IFR - Instrument Flight Rules
IMC - Instrument Meteorological Conditions
ISSP - Integrated Safety System Program
JHA - Job Hazard Analysis
LAHSO - Land and Hold Short Operations
LDR - Labor Distribution Reporting
LOB - Line of Business
MES - Multi-Linear Event Sequencing Tool
MLS - Microwave Landing System
MMS - Maintenance Management System
MORT - Management Oversight and Risk Tree
NAIMS - Analysis National Aviation Information Management System
NAS - National Airspace System
NASA - National Aeronautics and Space Administration

NASDAC - National Aviation Safety Data Analysis Center
NASTEP - NAS Technical Evaluation Program
Nav - Navigation
NCP - NAS Change Proposal
NexGen - Next Generation (e-mail) Messaging System
NFPO - National Flight Procedures Office
NIMS - NAS Infrastructure Management System
NMACS - Near Midair Collision System
NOTAMS - Notice to Airmen
NTSB - National Transportation Safety Board
OA - Operations Analysis
OEDS - Operational Error/Deviation System
OIG - Office of the Inspector General
ORM - Operational Risk Management
OSA - Operational Safety Assessment
OSHA - Occupational Safety and Health Administration
PANS-ATM - Procedures for Air Navigation Services, Air Traffic Management
PDR - Preliminary Design Review
PDS - Pilot Deviation System
PE - Physical Examination
PHA - Preliminary Hazard Analysis
POSC - Post-Implementation Safety Case
RIS - Regulatory Information System
RNP-RNAV - Required Navigation Performance for Area Navigation
RTCA - Radio Technical Commission for Aeronautics
RVSM - Reduced Vertical Separation Minima
SEM - System Engineering Manual
SID - Standard Instrument Departure
SMO - Systems Management Office
SMS - Safety Management System
SOIA - Simultaneous Offset Instrument Approach
SRM - Safety Risk Management
SRMD - Safety Risk Management Document

SSAR - System Safety Assessment Report
SSE - Senior Safety Engineer
SSH - System Safety Handbook
SSHA - Sub-system Hazard Analysis
SSMP - System Safety Management Program
STARS - Standard Terminal Automation Replacement System
STEP - Sequential Time Event Plot
T&E - Test and Evaluation
TAA - Terminal Arrival Area
TRACON - Terminal Radar Approach Control
UCR - Unsatisfactory Condition Report
VFR - Visual Flight Rules
VHF - Very High Frequency
VMC - Visual Meteorological Conditions
VOR - VHF Omni-directional Range
VP - Vice President
WBI - Web-based Instruction