Federal Aviation Administration

FAA SAFETY MANAGEMENT

SAFETY RISK MANAGEMENT GUIDANCE: THE 5 STEP PROCESS

AVP-300-003-JA1 (Version 2.0)
April 27, 2018

This document is located on the Federal Aviation Administration (FAA) Safety Management Intranet site as part of the Safety Risk Management Guidance. The document was developed by the FAA Safety Management System (SMS) Committee and is owned and maintained by the Safety Management and Research Planning Division (AVP-300) in the Aviation Safety Organization (AVS). For more information, individual contacts are listed on the contacts page on the site.

Federal Aviation Administration Safety Risk Management Guidance: The 5 Step Process
AVP-300-003-JA1

Purpose

The purpose of this document is to provide guidance on how to plan for Safety Risk Management (SRM) and conduct each of the five steps in the SRM process (System Analysis; Identify Hazards; Analyze Safety Risk; Assess Safety Risk; Control Safety Risk). Federal Aviation Administration (FAA)-level cross-organizational SRM is conducted in accordance with the current version of FAA Order 8040.4, Safety Risk Management Policy.

Scope

This guidance applies to all FAA organizations involved in conducting FAA-level, cross-Line of Business (LOB)/Staff Office SRM.

Approval: Paula Martens
FAA SMS Committee Chair

REVISION HISTORY

Revision Number	Description of Change	Effective Date
0	Original Document (Version 1.0)	August 12, 2015
1	Aligned document to Federal Aviation Administration (FAA) Order 8040.4B, *Safety Risk Management Policy*. Includes review by the Aviation Safety Safety Management System (AVSSMS) Coordination Group and FAA Safety Management System (SMS) Committee.	TBD

Table of Contents

SRM Process Overview

Safety Risk Management (SRM) is a formalized, proactive approach to system safety. It is a five-step process that provides a means to identify, analyze, assess, and control safety risk in the aerospace system. Hazards present conditions that affect operations in a way that result in degraded system performance, ultimately resulting in an unwanted outcome. A thorough understanding of the components of safety risk must include an examination of the factors that make system events (errors or failures) that can result in unwanted outcomes (accidents or incidents) more or less likely. The analysis must also consider the type of outcomes possible in order to estimate potential severity. As depicted in Figure 1, the 5 Step SRM process is continuous, meaning that processes are repeated until the safety risk associated with each hazard is acceptable.

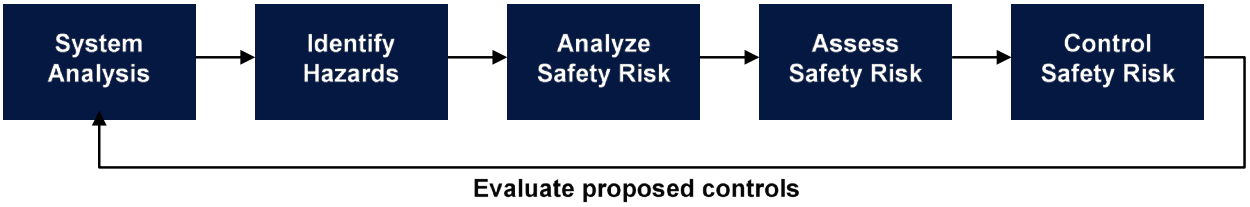

Figure 1: 5 Step SRM Process

Planning SRM

Planning is necessary before starting the analysis and may require the Office of Primary Responsibility (OPR) to:

- Define and document the scope (i.e., system boundaries) and objectives related to the system
- Identify appropriate stakeholders
- Coordinate with other organizations that may be affected by the issue/change or the risk mitigation strategies
- Identify an SRM team facilitator if a team is needed
- Identify a facility/organization/program/technical lead (i.e., Subject Matter Expert [SME])
- Work with the SRM team facilitator to clearly define the scope of the issue/change
- Document the issue/change information in the Hazard Identification, Risk Management and Tracking (HIRMT) tool, if applicable.
- Note: Per Federal Aviation Administration (FAA) Order 8040.4, *Safety Risk Management Policy*, Lines of Business (LOBs) and Staff Offices are responsible for identifying and tracking hazards within their purview. In addition, they are responsible for capturing and reporting the progress of identified Aerospace System Level (ASL) safety issues into HIRMT. While LOBs and Staff Offices can use their own tools to collect and maintain information regarding safety issues that are addressed wholly within their organization, if the safety issue meets the ASL criteria, the information must be entered into HIRMT.

The scope of the SRM effort is based on the type, complexity, and impact of the issue/change. It is critical that the level of detail in the safety analysis match the scope and complexity of the

issue/change. Further information regarding planning cross-LOB/Staff Office SRM efforts is detailed in the *Guidance for Coordinating Cross-LOB Safety Risk Assessments*.

Step 1: System Analysis

Overview

As part of the safety analysis, the SRM team must create a detailed description of the system in which the issue/change needs to be assessed. A complete and accurate system description is a critical foundation for conducting a thorough, unbiased safety analysis. The system analysis or system description provides information that serves as the basis for identifying and understanding hazards, as well as their causes and associated safety risks. When describing and analyzing the system, it is critical that the OPR and SRM team members:

- Agree to the scope (i.e., system boundaries) and objectives related to the system that was discussed during the SRM planning
- Gather the relevant available data/information regarding the issue or change to be analyzed. This includes available incident/accident data; previous applicable analyses and assessments; and related requirements, rules, and regulations, as necessary.
- Develop a safety risk acceptance plan that includes evaluation against safety risk acceptance criteria, designation of authority to make the required safety risk decisions involved, and assignment of the relevant decision makers, ensuring consistency with the safety risk acceptance criteria and risk matrices and definitions in FAA Order 8040.4, *Safety Risk Management Policy*. Some parts of the risk acceptance plan may need to be updated based on the results of later steps in the process (for instance, the designation of authority to make risk acceptance decisions may need to be updated depending on the proposed safety risk mitigations).
- Describe and model the system and operation in sufficient detail for the SRM Team members and safety analysts to understand and identify the hazards that can exist in the system, as well as their sources and possible outcomes. One example of modeling is creating a functional flow diagram to help depict the system and the interface with the users, other systems, or sub-systems.
- Look at the system in its larger context, including how the system may change over time. A system is often a subcomponent of some larger system(s). Therefore, a change to a system could affect the interfaces with these systems. SRM should address the effects on the interfaces or other systems and/or coordinate with the owners of those other systems. For example, a change to the design of an aircraft may affect the maintenance and/or operation of that aircraft.

When describing the system, the following should be considered, as appropriate, depending on the nature and size of the system:

- Function and purpose of the system/item being assessed
- Interactions with other systems and sub-systems in the broader aerospace system
- Personnel, equipment (e.g., hardware and software components), and facilities necessary for the system's operation
- Human factors requirements (e.g. cognitive, ergonomic, environmental, etc.) for operations, and maintenance
- The system's processes, procedures, and performance

- Related procedures that define guidance for the operation and use of the system/item being assessed
- Ambient environment
- Operational environment
- Maintenance environment
- Contracted and purchased products and services
- The interactions between the items listed above
- Any assumptions made about the system/item being assessed and its interactions in the aerospace system
- Existing safety risk controls

Potential Effects on the System or Interfacing Systems

During the System Analysis step in the SRM process, the SRM team considers all critical factors for that specific safety issue as determined by the SMEs. The resulting description defines the scope of the risk assessment. A complete and accurate system description is the foundation for conducting a thorough safety analysis. System descriptions need to exhibit two essential characteristics—correctness and completeness.

- Correctness means that the system description provides an accurate reflection without ambiguity or error.
- Completeness means that nothing has been omitted and that everything stated in the system description is essential and appropriate to the necessary level of detail.

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

- What is the purpose of the system or change?
- How will the system or item be used?
- What are the system or item functions?
- What are the system or item boundaries and external interfaces?
- What is the environment in which the system or change will operate?
- What are the interconnectivity and/or interdependencies between systems?
    - Does the system provide source material as input to external National Airspace System (NAS) systems?
    - Does the system receive source material as input from external NAS systems?
    - Does the system create or require any functional interdependencies on or from external NAS systems?
    - Will the system impact or cause external NAS legacy systems to change the way they currently function (e.g., levying new requirements as a result of the change)?
- How will the issue/change impact system users?
- What existing risk controls are present in the system or change?

The following are examples of data that the SRM team could consider when describing the system:

- Average annual approaches to each runway
- Number of hours the airport is at or below minimums
- Number and type of airport operations
- Number of aircraft controlled, ground, pattern, Instrument Flight Rules (IFR), Visual Flight Rules (VFR), and transitions
- Number of hours the airport is in VFR vs. IFR
- Design information including availability and reliability for both hardware and software
- Number of pilot deviations
- Number of Mandatory Occurrence Reports (MORs)/ Electronic Occurrence Reports (EORs)
- Number of pedestrian/vehicle deviations
- Accident/injury data

System Description Models

The SRM team can use a variety of methods to create a system description. The 5M Model is one useful method to capture the information needed to describe the system. Another method is the SHELL Model. The SRM Tools guidance document contains additional information regarding system description and analysis models.

The SRM team uses these models and similar techniques to deconstruct the issue/change to distinguish elements that are part of, or impacted by, the issue/change. These elements later help to identify sources, causes, hazards, and current and proposed hazard mitigations.

Bounding the System and Depth and Breadth of the Analysis

Bounding is limiting the safety analysis to the elements that affect or interact with each other to accomplish the central function. The level of detail in the description varies, typically proportionally to the breadth of the issue/change.

The system description has both depth and breadth. The depth and breadth of the analysis necessary for SRM varies. The breadth of a system analysis refers to the system boundaries. Depth refers to the level of detail in the description. Some of the factors used to determine the depth and breadth of the analysis include:

- **The size and complexity of the issue/change under consideration** – A larger and more complex issue/change may also require a larger and more complex analysis.
- **The breadth of an issue/change** – SRM scope can be expected to increase if the issue/change spans more than one organization, service/office, or LOB/Staff Office.
- **The type of issue/change** – Technical issues/changes tend to require more analysis than non-technical issues/changes. For example, procedural- or equipment-driven issues/changes tend to require more analysis than changing document requirements or a radio frequency.

When selecting the appropriate depth and breadth of the safety analysis, multiple factors must be considered. In general, safety analyses on more complex and far-reaching items will require a greater depth and breadth. For example, a major acquisition program could require multiple safety analyses involving hundreds of pages of data at the preliminary, sub-system, and system levels, evaluating numerous interfaces with other systems, users, and maintainers in the aerospace system. However, an analysis of an operational procedure may require a less intensive analysis. In both cases, the SRM requirements are met, but the safety analysis is

tailored to meet the needs of the decision-makers. In general, the level of detail in the description varies inversely with the breadth of the system.

A primary consideration in determining both depth and breadth of the safety analysis is: What information is required to know enough about the issue/change, the associated hazards, and each hazard's associated risk to choose which controls to implement and whether to accept the risk? The scope of the analysis enables the SRM Team to make an informed decision about the acceptability of risk. The role of the SRM team is to objectively examine potential hazards and effects associated with any system changes. If there is doubt about whether to include a specific element in the analysis, it is better to include that item at first, even though it might prove irrelevant during the hazard identification step.

Guidelines to help determine the scope of the safety analysis include:

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

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

- More complex and/or increased quantity of functions may increase the number of hazards and related causes.
- Complex and detailed analyses may explore multiple levels of hazard causes, sometimes in multiple safety analyses.
- Hazards that are suspected to have associated initial high or medium risk should be thoroughly analyzed for causal factors and likelihood.
- The analysis should be conducted at a level that can be measured or evaluated, whereas the limitations of data availability may necessitate a less quantifiable approach and/or result than when data is available.

A thorough system description and the elements within it constitute the potential sources of hazards associated with the issue/change. This is necessary for the subsequent steps of the SRM process. The resulting bounded system description limits the analysis to the components necessary to adequately assess the safety risk.

Step 2: Identify Hazards

Overview

Once the system has been completely and accurately described (Step 1), the SRM team identifies hazards. A hazard is defined as is a condition that could foreseeably cause or contribute to an accident. A thorough system description contains the potential sources of hazards. During the hazard identification step, the SRM team identifies and documents hazards, their possible causes, and corresponding outcomes. The level of detail required in the hazard identification process depends on the complexity of the issue/change being considered

and the stage at which the analysis is performed. A more comprehensive hazard identification process typically leads to a more rigorous safety analysis.

Elements of Hazard Identification

The SRM team needs the following to identify hazards:

- Operational expertise
- Training or experience in various hazard analysis techniques
- A defined hazard analysis tool

The SRM team must also identify data sources and measures, which are necessary to identify hazards and to monitor for compliance with mitigation strategies. Data monitoring also helps detect hazards that are more frequent or more severe than expected or mitigation strategies that are less effective than expected. The SRM team selects the tool that is most appropriate for the type of system being evaluated. The SRM Tools guidance document contains tools/ methods used for identifying hazards.

Potential Sources of Hazards

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

- Ambient environment (physical conditions, weather, etc.)
- Equipment (hardware and software)
- External services (contract support, electric, telephone lines, etc.)
- Human-machine interface
- Human operators
- Maintenance procedures
- Operating environment (airspace, air route design, etc.)
- Operational procedures
- Organizational culture
- Organizational issues
- Policies/rules/regulations

The elements in the system description are the sources for hazards. More information on potential sources of hazards is included in the section on Defenses in Depth in Step 5. For software safety in FAA acquisitions, please refer to the SRM Guidance for System Acquisitions (SRMGSA) for guidance.

Causes, System State, and Effect

During the hazard identification step, the SRM team identifies and documents hazards, their possible causes, the conditions (or system state) under which hazards might be realized, and their corresponding effects. Note that a single hazard can have multiple effects.

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

- Human error
- Latent errors
- Design flaws

- Component failure
- Software errors
- Ambient conditions

A system state is defined as the expression of the various conditions, characterized by quantities or qualities in which a system can exist. It is important that the SRM team capture the system state that most exposes a hazard. The system description remains within the confines of any operational conditions and assumptions defined in existing documentation. System state can be described using one or some combination of the following terms:

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

Any given hazard may have a different risk level in each possible system state, or even not exist in every system state. Hazard assessment must consider all possibilities while allowing for all system states. In a hazard analysis, it is important to capture different system states when end results lead to the application of different mitigations.

The SRM team should also address the accumulation of “minor” failures or errors that result in hazards with greater severity or likelihood than would result if each were considered independently. The effect is a description of the potential outcome or harm of the hazard if it occurs in the defined system state.

The Hazard Model section below contains more information on the relationship between causes, hazards, events, and outcomes.

Hazard Model

For the purpose of SRM, one needs to understand the scenario that reveals how adverse outcomes can occur in order to perform the analysis and develop any subsequent risk controls. The hazard model shown in Figure 2 was developed to ensure that the necessary components for the risk analysis are understood and identified while applying the SRM process.

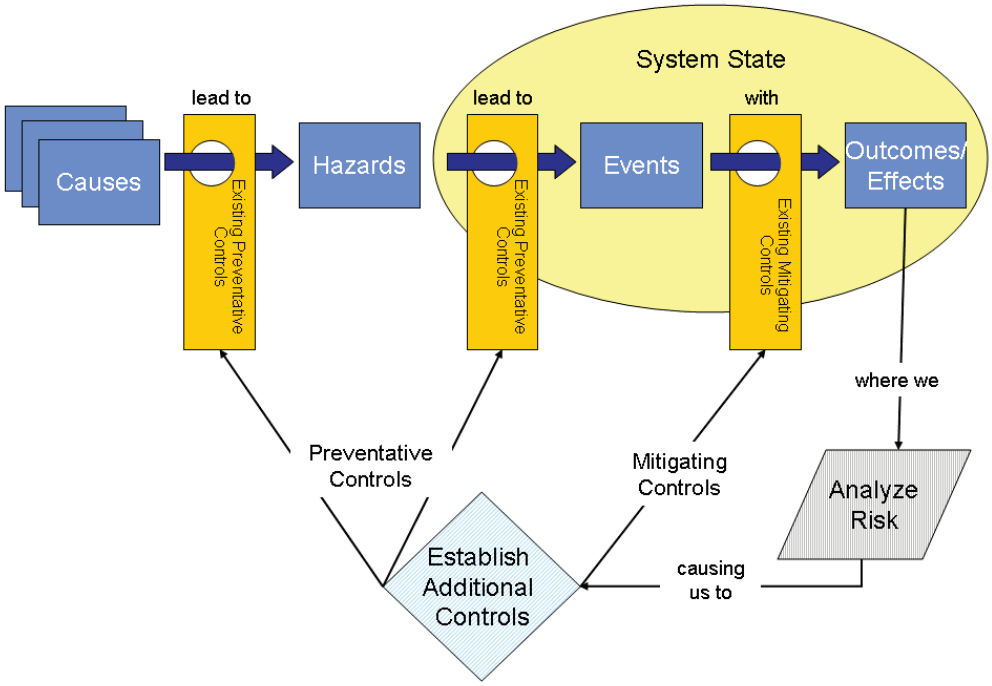

Figure 2: Hazard Model

As defined in the current version of FAA Order 8040.4, *Safety Risk Management Policy*, a hazard is a condition that could foreseeably cause or contribute to an accident. Hazard identification must consider all credible possibilities, from the least to the most likely. Credible means that it is reasonable to expect the existence of the hazard. The hazards to be included in the final analysis must be credible hazards considering all applicable existing controls.

It is possible, and often necessary, to identify the causes of hazards or the element of the system that enables the hazard to exist. This may be useful to understand the nature of the issue/item and development of risk controls if necessary. However, each cause of a hazard may have its own cause. It is up to the SRM team to evaluate the necessity of determining the causes.

As illustrated in Figure 2, there are two types of risk controls. Preventative risk controls are designed-in barriers to prevent the propagation of a hazard to an event. Mitigating risk controls typically focus on mitigating the adverse outcome after the event occurs. When determining how a hazard can lead, or has led, to an event, existing risk controls must be considered. An adverse outcome may be the result of an ineffective preventative risk control and not necessarily due to a new hazard not previously identified. An adverse outcome may also be the result of a new hazard not already identified or resulting from a change to the system, for which no preventative risk controls exist.

An adverse safety outcome occurs when the set of existing safety risk controls is inadequate or ineffective. An event can be characterized as when the system deviates from the expected operation or intended function. Not all events will lead to an adverse outcome, but there is potential that an adverse outcome could occur. In addition, potential outcomes/effects are affected by the system state. System state is defined as the expression of the various

conditions, characterized by quantities or qualities in which a system can exist. It is important to consider all system states to identify outcomes and unique mitigations. The various system states in which the hazard exists should be identified because the risk of the outcome may be different based on the system state. For example, an event may lead to an adverse outcome in the landing phase of flight but not while in cruise.

The SRM Tools guidance document provides numerous tools (e.g., the Bow-Tie model and Root Cause Analysis) that can help illustrate the relationship between causes, hazards, and what kind of environment (system state) enables their propagation into the different outcomes/effects.

Step 3: Analyze Safety Risk

Overview

In this step, the SRM team determines the severity and likelihood of each adverse safety event by:

- Evaluating each hazard identified in Step 2 based on the system state in which it potentially exists and what controls exist to prevent or reduce the hazard's occurrence or effect(s)
- Comparing a system and/or sub-system performing its intended function in anticipated operational environments, to those events or conditions that would reduce system operability or service; the events may, if not mitigated, continue until total system degradation and/or failure occurs

Once the SRM team documents the mitigations, also called existing controls, it estimates the hazard's risk.

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

Risk is defined as the composite of predicted severity and likelihood of the potential effect of a hazard. The SRM team can use quantitative or qualitative methods to analyze the risk. Different failure modes of the system(s) can impact both severity and likelihood in unique ways.

Existing Controls

It is important to document existing controls because they impact the ability to establish severity and likelihood determinations. When identifying existing controls, one accounts for controls specific to the change, hazard, and system state. A control can only be considered existing if it has been confirmed with objective evidence. Table 1 provides some examples of existing controls.

Table 1: Existing Control Examples

Controller	Pilot	Equipment/Technical Operations

• Radar Surveillance
  − Ground and Airborne
• Controller Scanning
  − Radar
  − Visual (Out Window)
• Conflict Alert (CA), Minimum Safe Altitude Warning (MSAW), Airport Movement Area Safety System (AMASS) Airport Surface Detection Equipment – Model (ASDE-X)
• Procedures
  − Specific Standard Operating Procedure (SOP) Reference
  − FAA Order Reference
• Triple Redundant Radio
• Controller Intervention
• Training
  − Implementation
  − Routine Periodic
• Management Oversight
	• Traffic Alert and Collision Avoidance System (TCAS)
	• Ground Proximity Warning System (GPWS)
	• Visual Scanning (Out Window)
	• Radar Surveillance
	  − Airborne
	• Checklists
	• Redundancies/Back-up Systems
		• Preventative Maintenance
		• Failure Warnings/Maintenance Alerts
		• Redundancy Systems
		  − Triple Redundant Radio
		  − Software Redundancy
		• Diverse Points of Delivery
		  − Microwave and Telecommunications
		• Fall Back Systems
		  − Center RADAR Processing (CENRAP)
		  − Direct Access RADAR Channel (DARC)
		• Software/Hardware Design

Determining Severity

Severity is the potential consequence or impact of a hazard in terms of degree of loss or harm. It is a prediction of how bad the outcome of a hazard can be. There may be many outcomes associated with a given hazard, and the severity should be determined for each outcome. One does not consider likelihood when determining severity; determination of severity is independent of likelihood. The goal of the safety analysis is to define appropriate mitigations for the risk associated with each hazard. It is important that the SRM team consider all possible outcomes in order to identify the highest risk and develop effective mitigations for each unique outcome.

The following table contains generic severity definitions as provided in the current version of FAA Order 8040.4, *Safety Risk Management Policy*. LOBs/Staff Offices may use more specific definitions in their application of SRM or define severity in quantitative terms such as fatal accidents. The definitions are not meant to imply a specific point, but instead, convey a spectrum across the cells from very low to very high. Additionally, even within each cell there is a range of severities which lies between the ranges described in the cells before and after it.

Table 2: Severity Definitions

Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Negligible safety effect	• Physical discomfort to persons • Slight damage to aircraft/vehicle	• Physical distress or injuries to persons • Substantial damage to aircraft/vehicle	Multiple serious injuries; fatal injury to a relatively small number of persons (one or two); or a hull loss without fatalities	Multiple fatalities (or fatality to all on board) usually with the loss of aircraft/ vehicle

*Excludes vehicles, crew, and participants of commercial space flight.

Determining Likelihood

Likelihood is the estimated probability or frequency, in quantitative or qualitative terms, of the outcome(s) associated with a hazard. That is, it is an expression of how often one expects an outcome to occur in the future.

The SRM team needs to consider severity in conjunction with the determination of likelihood, in order to predict an accurate risk score. Likelihood is determined by how often one can expect the resulting harm of an outcome to occur. The following tables contain generic likelihood definitions, separated by categories of operations, as provided in the current version of FAA Order 8040.4, *Safety Risk Management Policy*. LOBs/Staff Offices may use more specific definitions in their application of SRM or base likelihood in probabilistic terms. The definitions are not meant to imply a specific point, but instead, convey a spectrum across the cells from very low to very high. Additionally, even within each cell there is a range of likelihood which lies between the ranges described in the cells before and after it.

Table 3: Likelihood Definitions for Commercial Operations/Large Transport Category

	Qualitative	Quantitative – Time/Calendar-based Occurrences Domain-wide/System-wide
Frequent A	Expected to occur routinely	Expected to occur more than 10 times per year
Probable B	Expected to occur often	Expected to occur between one and 10 times per year
Remote C	Expected to occur infrequently	Expected to occur one time every 1 to 3 years
Extremely Remote D	Expected to occur rarely	Expected to occur one time every 3 to 10 years
Extremely Improbable E	Unlikely to occur, but not impossible	Expected to occur less than once every 10 years

Table 4: Likelihood Definitions for General Aviation Operations/Small Aircraft and Rotorcraft

	Qualitative	Quantitative – Time/Calendar-based Occurrences Domain-wide/System-wide
Frequent A	Expected to occur routinely	Expected to occur more than 100 times per year (or more than approximately 10 times a month)
Probable B	Expected to occur often	Expected to occur between 10 and 100 times per year (or approximately 1-10 times a month)
Remote C	Expected to occur infrequently	Expected to occur one time every 1 month to 1 year
Extremely Remote D	Expected to occur rarely	Expected to occur one time every 1 to 10 years
Extremely Improbable E	Unlikely to occur, but not impossible	Expected to occur less than one time every 10 years

Use of Qualitative and Quantitative Data

The scientific method relies on both quantitative and qualitative data. The quantitative data can provide a solid calculation of overall risk, where qualitative observations can ground the data to real-world situations. The most effective safety risk analyses contain both types of data. Using quantitative data is preferred, as it tends to provide more objective results; however, when quantitative data is not available, it is acceptable to rely on qualitative information and expert judgment. Qualitative judgment varies from person to person, so if only one person is performing the analysis, the result should be considered an opinion. With a team of experts involved in the analysis, one can consider the result qualitative data or expert judgment.

Characteristics of quantitative data include:

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

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

Characteristics of qualitative data include:

- Data are expressed as a measure of quality
- Data are subjective

- Data allow for examination of subjects that can often not be expressed with numbers but by expert judgment

In qualitative analysis, the intellectual and intuitive judgment of the analyst(s) is the most important factor in the analysis and its outcome. Qualitative techniques work best when analyzing a conceptual entity where data and knowledge on which to base a numerical analysis are absent or unobtainable and the results are only needed to make a decision related specifically to the issue/item under study.

Quantitative analysis is best suited to cases where the phenomena under study can be modeled mathematically and data exist that will support that model. This type of analysis tends to minimize subjective analytical variation, and is suitable for situations in which results of separate analyses must be compared on an equal basis and decisions made based on those comparisons. It is also best when there are specific numerical risk thresholds or guidelines against which the risk is compared to justify specific risk exposure timeframes. Such analytical methods require that the analyst be mathematically knowledgeable in proportion to statistical aspects of the analysis being performed and knowledgeable enough about the phenomenon being analyzed to make the qualitative judgments that invariably remain.

Step 4: Assess Safety Risk

Overview

In the Assess Safety Risk step, the SRM team:

- Compares each hazard's associated risk per outcome (as identified in Step 3) against the risk acceptance plan developed in Step 1
- Determines which outcomes associated with the hazard represent high, medium, and low risk
- Determines the need for risk control development based on level of risk

Risk Matrix

A risk matrix is a graphical means of determining safety risk levels that may be used in the SRM process. The columns in the matrix reflect previously introduced severity categories; its rows reflect previously introduced likelihood categories. The risk matrices provided in the current version of FAA Order 8040.4, *Safety Risk Management Policy* are intended as a standardized baseline to facilitate communication across FAA organizations.

Some FAA organizations have existing safety risk assessment processes to determine safety risk levels without using a risk matrix (for example, evaluation against the probability of a fatal outcome). Since there is obvious overlap, the risk matrix may be useful in communication between LOBs/Staff Offices. The risk matrix is a tool that facilitates communication regarding safety risk among the FAA organizations through the graphical illustration of safety risk analysis and assessment results.

Using the risk matrix across the LOBs/Staff Offices does not preclude organizations from using their own means of analyzing and assessing safety risk. It also does not preclude organizations from using methodologies or frameworks other than the risk matrix to illustrate and communicate the results of those analyses and assessments within an LOB/Staff Office. Therefore, if a hazard, its associated safety risk, and safety risk controls stay within an

LOB/Staff Office, the LOB/Staff Office may use its existing safety risk assessment methodology. It does not have to translate its assessment into the risk matrices included in FAA Order 8040.4.

When the team conducting the analysis is composed of members from LOBs and Staff Offices that use different risk matrices, the team uses the risk matrices in FAA Order 8040.4, unless all stakeholder FAA organizations agree to use a different method or tool.

Types of Risk

- **Initial risk** is the predicted severity and likelihood of a hazard's effects or outcomes when it is first identified and assessed; it includes the effects of preexisting safety risk controls in the current environment.
- **Residual risk** is the remaining predicted severity and likelihood that exists after all selected safety risk control techniques have been implemented.

Ranking and Prioritizing Risk for Each Hazard

The risk levels, according to FAA Order 8040.4, used in the process are defined below.

- **High Risk** – Severity and likelihood map to the red cells in the risk matrix. This safety risk requires mitigation, tracking, and monitoring, and it can only be accepted at the highest level of management within LOBs and Staff Offices.
- **Medium Risk** – Severity and likelihood map to the yellow cells in the risk matrix. This safety risk is acceptable without additional mitigation; however, tracking and monitoring are required.
- **Low Risk** – Severity and likelihood map to the green cells in the risk matrix. This safety risk is acceptable without restriction or limitation; hazards are not required to be actively managed, but they must be documented and reported if a safety risk assessment has been performed.

Using the risk matrix, the SRM team ranks and prioritizes each outcome of a hazard according to its associated safety risk levels following the steps below:

- When appropriate, rank hazard outcomes according to their associated safety risk levels (illustrated by where they fall on the risk matrix).
- To plot a hazard outcome on the risk matrix, select the appropriate severity column (based on the severity definitions) and move down to the appropriate likelihood row (based on the likelihood definitions).
- Plot the hazard outcome in the box where its severity and likelihood meet.
- If this box is red, the safety risk associated with the hazard outcome is High; if the box is yellow, the safety risk associated with the hazard outcome is Medium; if the box is green, the safety risk associated with the hazard outcome is Low.
- Select the initial/current risk based on the severity and likelihood selections made.

Figures 3 and 4 show the risk matrices in the current version of FAA Order 8040.4

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

High Risk [Red]

Medium Risk [Yellow]

Low Risk [Green]

* High Risk with Single Point and/or Common Cause Failures

Figure 3: Risk Matrix – Commercial Operations/Large Transport Category

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

High Risk [Red]

Medium Risk [Yellow]

Low Risk [Green]

* High Risk with Single Point and/or Common Cause Failures

Figure 4: Risk Matrix – General Aviation Operations/Small Aircraft and Rotorcraft

- In Figure 3 (Risk Matrix for Commercial Operations/Large Transport Category), a catastrophic severity and corresponding extremely improbable likelihood qualify as yellow risk in the split cell in the bottom right corner of the matrix, as long as the effect is not the result of a single point or common cause failure. If the cause is a single point or common cause failure, the effect of the hazard is categorized in the red part of the split cell in the bottom right corner of the matrix.
    - A **single point failure** is defined as a failure of an element of a system or operation for which no backup (i.e., redundancy) exists. Single-pilot operations are an exception. An example of a single point failure is a single fuel line, which if clogged could result in the loss of engine power in an aircraft.
    - A **common cause failure** is defined as a failure that occurs when a single fault results in the corresponding failure of multiple system components or functions. An example of a common cause failure is redundant computers running on the same software, which is susceptible to the same software bugs.
- In Figure 4 (Risk Matrix for General Aviation Operations/Small Aircraft and Rotorcraft), a catastrophic severity and corresponding extremely remote likelihood qualify as yellow risk in the split cell in the matrix, as long as the effect is not the result of a single point or common cause failure. If the cause is a single point or common cause failure, the effect of the hazard is categorized in the red part of the split cell in the matrix.
- Once mitigations are developed and the analysis is conducted taking into account those mitigations, the residual risk is plotted. Plotting the prediction of the residual risk illustrates the impact of the safety risk controls on the initial risk and shows the decision-maker whether or not the safety risk associated with the hazard will be mitigated to an acceptable level.

Ranking the safety risk associated with the identified hazards prioritizes mitigation.

Step 5: Control Safety Risk

Overview

In this step, the SRM team develops and manages options to deal with risk (from Step 4). Effectively mitigating risk involves:

- Identifying feasible mitigation options
- Developing a risk mitigation plan and accepting the predicted residual risk
- Developing a monitoring plan detailing review cycles for evaluating the effectiveness of mitigations
- Implementing and confirming the mitigations

Monitoring the effectiveness of the mitigation is typically accomplished through safety assurance functions.

In the control safety risk step, the SRM team develops options for managing the risk associated with a hazard. These options become actions that reduce the risk of the hazard's effects on the system (e.g., human interface, operation, equipment, procedures). Regardless of who develops options to mitigate risk, safety risk controls established by the FAA must be approved by the FAA management officials who are responsible for their implementation and effectiveness before safety risk can be accepted. Note that the management officials who approve the safety

risk controls may be the same management officials who accept the safety risk, but this is not always the case.

Risk mitigation options should contain sufficient detail to allow their impact on the safety risk to be assessed. Note that there may be situations in which detailed risk control options cannot be developed without further research or assistance from industry. However, assumptions can be made and documented regarding possible risk control options. These assumptions should be considered in the risk monitoring plan and are often the subject of research and development activities.

The following are conceptual examples of risk control options:

- Avoiding the risk and/or removing the hazard by discontinuation of the activity/process/design that generates the unacceptable risk
- Decreasing the likelihood of the hazard leading to the adverse outcome(s)
- Reducing the severity of the associated outcome(s)
- Implementing barriers that prevent or minimize the outcome(s)

Strategies for Managing Risk

Risk mitigation requires management's informed decision to approve, fund, schedule, and implement one or more risk mitigation strategies. The objective of the Control Safety Risk step is to implement appropriate plans to mitigate the risk associated with identified hazards and their effects. Therefore, appropriate risk mitigation strategies are developed, documented, and recommended. The risk mitigation approach selected may fall into one or more of the following categories:

- Risk transfer strategy
- Risk avoidance strategy
- Risk control strategy

Once the risk mitigation strategies are selected and developed, management can identify the impact on other organization(s) and coordinate/obtain agreement on those strategies with the affected organization(s). In addition, a monitoring plan is established to ensure that risk mitigation strategies are effective. The risk mitigation process is repeated until risk is reduced to an acceptable level. Hazard tracking is a key element of this risk management step.

Risk Transfer

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

Examples of risk transfer may include:

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

- Transfer of Air Traffic Control (ATC) systems from the acquisition organization to the organization that provides maintenance

The receiving organization may be better equipped to mitigate the risk at the operational or organizational level. Transfer of risk, while theoretically an acceptable means of mitigating risk, cannot be the only method used to mitigate high risk associated with a hazard. The safety risk must still be mitigated to medium or low before it can be accepted in the aerospace system. In addition, when hazards (and their associated risk) that are typically outside the scope of the FAA Safety Management System (SMS) are identified (e.g., Occupational Safety and Health Administration [OSHA], physical security, etc.), organizations transfer the management and mitigation of risk to the appropriate organization.

Risk Avoidance Strategy

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

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

Risk Control Strategy

A control is a characteristic of a system that reduces safety risk. A control can also be described as anything that mitigates the risk of a hazard’s occurrence or effects. Controls may include process design, equipment modification, work procedures, training, or protective device. A control is the same as a safety requirement. All controls must be written in requirement language.

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

Risk Control Definition

A risk control is a means to reduce or eliminate the effects of hazards. Examples of safety risk controls include revising the system design, modifying operational procedures, training, and limitation of certain activities.

When risk is determined to be unacceptable, safety risk controls that would reduce the risk to an acceptable level are identified and evaluated. Once identified, the SRM team assesses the effect of the proposed safety risk control(s) on the overall risk. If necessary, the team repeats the process until a combination of measures reduces the risk to an acceptable level.

When risk mitigation strategies cross LOBs/Staff Offices, the stakeholder organizations must approve documentation and accept risk. The OPR is responsible for obtaining necessary approvals for the acceptance of risk. If the risk does not meet the pre-determined acceptability criteria, it must always be reduced to a level that is acceptable, using appropriate mitigation procedures. Even when the risk is classified as acceptable, if any measures could further reduce the risk, the appropriate party should:

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

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

Defenses in Depth

Designing an Error Tolerant System

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

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

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

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

Design attributes of an error tolerant system include:

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

For an accident to occur in a well-designed system, these gaps must develop in all of the defensive layers of the system at the critical time when that defense should have been capable of detecting the earlier error or failure. Figure 5 illustrates how an accident event must penetrate all defensive layers follows.

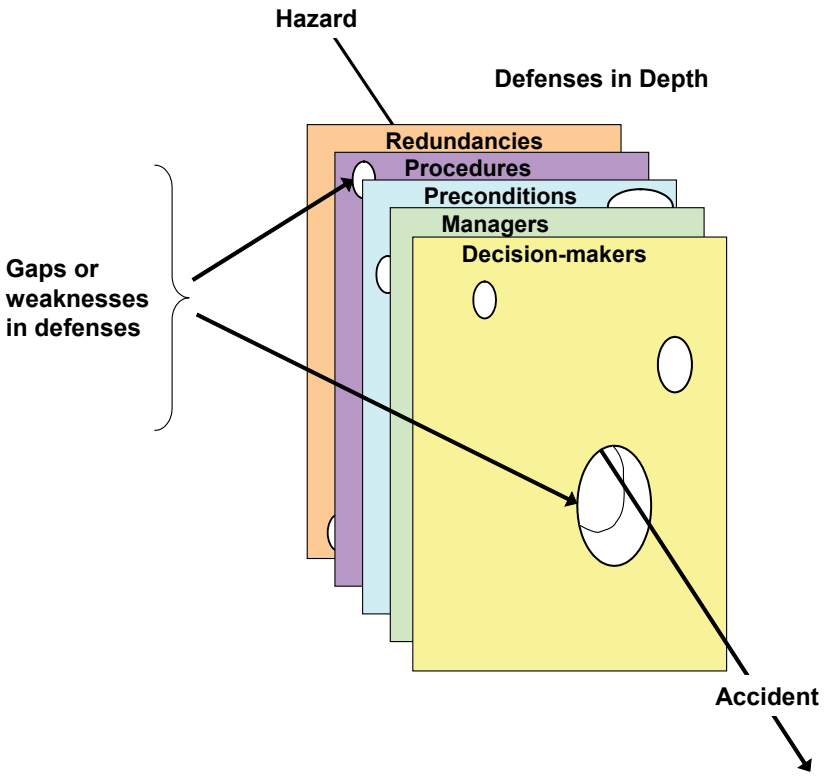

Figure 5: Defenses in Depth Philosophy

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

A latent failure is considered a failure that is not inherently revealed at the time it occurs. For example, when there is a slowly degrading back-up battery that has no state-of-charge sensor, the latent failure would not be identified until the primary power source failed and the back-up battery was needed. If no maintenance procedures exist to periodically check the battery, the failure would be considered an undetected latent event.

Detecting Gaps

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

Closing Gaps

Safety risk can be reduced proactively and reactively. Monitoring data/information, carefully analyzing the system, and reporting safety issues make it possible to proactively detect and prevent sequences of events where system deficiencies (i.e., faults and errors, either separately

or in combination) could lead to an incident or accident before it actually occurs. The same approach also can be used to reactively analyze the chain of events that led to an accident or incident. With adequate information, safety professionals can take corrective action to strengthen the system's defenses when devising new procedures, operations, and equipment, or when making changes to them. The following examples of typical defenses used in combination to close gaps are illustrative and by no means a comprehensive list of solutions.

Equipment

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

Operating Procedures

- Adherence to standard phraseology and procedures
- Readback 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, receiving immediate coordination from the handing-off sector)
- Inclusion of a validity indicator in designators for Standard Instrument Departures and standard terminal arrival routes
- Training, analyses, and reporting methods

Organizational Factors

- Management commitment to safety
- Current state of safety culture
- Clear safety policy implemented with adequate funding provided for safety management activities
- Oversight to ensure correct procedures are followed
- No tolerance for willful violations or shortcuts
- Adequate control over the activities of contractors

<u>Effect of Hardware and Software on Safety</u>

System designers generally design the hardware and software components of a system to meet specified levels of reliability, maintainability, and availability (note that just having high reliability, maintainability, and availability does not necessarily guarantee a safe system). The techniques for estimating system performance in terms of these parameters are well established. When necessary, system designers can build redundancy into a system, to provide alternatives in the event of a failure of one or more elements of the system.

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

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

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

Human Element's Effect on Safety

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

- Sense modalities (manner and ability of the senses, [e.g., seeing, hearing, touching])
- Cognitive functioning
- Reaction time
- Physical size and shape
- Physical strength

Fatigue, illness, and other factors such as stressors in the environment, noise, and task interruption also impact human performance. Designers use Human Error Analysis (HEA) to identify the human actions in a system that can create hazardous conditions. Optimally, the system is designed to resist human error (error resistant system) or at a minimum, to tolerate human error (error tolerant system).

People make errors, which have the potential to result in an adverse outcome. Accidents and incidents often result from a chain of independent errors. For this reason, system designers must design safety-critical systems to eliminate as many errors as possible, minimize the effects of errors that cannot be eliminated, and lessen the negative impact of any remaining potential human errors.

Within the FAA, human factors is defined as a "multidisciplinary effort to generate and compile information about human capabilities and limitations and apply that information to equipment, systems, facilities, procedures, jobs, environments, training, staffing and personnel

management for safe, comfortable, effective human performance" (FAA Order 9550.8, *Human Factors Policy*).

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

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

Safety Order of Precedence

One of the fundamental principles of system safety is the Safety Order of Precedence in eliminating, controlling, or mitigating a hazard. Safety professionals use the techniques listed in the Safety Order of Precedence, in priority order, for reducing risk. The SRM Tools guidance document provides information on the Safety Order of Precedence.

Evaluate Proposed Controls

Once the risk controls are developed, the steps of the SRM process are followed again to ensure that the safety risk has been sufficiently reduced. Further analysis is performed to ensure that no new hazards have been introduced or that existing safety risk controls have not been compromised based on the proposed safety risk controls. If the residual risk is not acceptable, the proposed safety risk controls are redesigned or new safety risk controls are developed as necessary and the analysis is conducted again.

When the associated risk cannot be reduced to an acceptable level after attempting all possible mitigation measures, then the safety requirements have not been satisfied. Therefore, the original objectives must be revisited or the proposal must be abandoned. If the proposal is unacceptable, the system or change cannot be implemented. This conclusion must be included in the SRM documentation.

Safety Performance Measures

Safety performance measures are measurable goals used to confirm the predicted residual risk of a hazard. They should quantifiably define the predicted residual risk. The SRM team defines the hazard's safety performance measure when it defines the mitigation strategy and assesses the predicted residual risk. The sources of data used for SRM team research should also be evaluated when developing safety performance measures. The SRM team data analysis serves as the basis for comparison against the post-implementation metrics.

The SRM team should not define the effects producing the highest risk level as the safety performance measure; instead, the SRM team should look at the less severe effects or indicators. An SRM team must define the safety performance measures in order to confirm the safety risk controls have the desired effect.

Developing a Control Implementation/Monitoring Plan

As part of the SRM documentation, the SRM team develops a control implementation/ monitoring plan. This plan is established to:

- Confirm the risk controls have been implemented and have the desired effect
- Enable monitoring of the effectiveness of those controls
- Confirm safety performance measures are met

It may also be used to conduct post-implementation assessments to verify the results of the analysis. Table 5 shows a sample Recommended Control Implementation/Monitoring Plan.

Table 5: Sample Recommended Control Implementation/Monitoring Plan

Task	Responsible	Due Date/ Frequency	Status/Measure
Implementation of Controls			
The recommended mitigation that was designed for the change	Individual, division, or organization required to render account concerning the identified task	The date by which the responsible party must have completed the identified task	The state of the task
Example: Safety device X will be installed in Equipment Z.	Example: ZDC Technicians	Example: December 5, 2010	Example: Open*
Monitoring			
A function to be performed; an objective	Individual, division, or organization required to render account concerning the identified task	The frequency and duration that the task will be performed	The state of the task including any safety performance measures and a statement regarding the initial risk and the predicted residual risk
Example 1: Internal audit of the maintenance records	Example 1: Quality Assurance Office	Example 1: Monthly, quarterly, etc.	Example 1: Ongoing*, Closed
Example 2: Track and monitor availability of equipment Z to users	Example 2: Quality Assurance Office	Example 2: Monthly, quarterly, etc.	Example 2: Safety performance measure is 98% availability

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

Safety professionals may conduct post-implementation assessments for the life of the system or change, as defined in the monitoring plan, which is documented in the SRM documentation. The frequency of assessments depends on the type, the potential safety impact, and/or the complexity of the change, as well as the depth and breadth of the original analysis. Existing support mechanisms should be considered in post-implementation assessments, after which the SRM documentation is updated. These support mechanisms may include Independent Operational Test and Evaluation (IOT&E), Flight Inspection, the Air Traffic Evaluation and Auditing Program, National Airspace System Technical Evaluation Program (NASTEP), SRM audits of manufacturing facilities and air carriers, monitoring of various type certifications, and

collection and analysis of incident and accident data. Safety Assurance is the general method of monitoring safety and is used to determine if new hazards have been identified, ineffective controls exist, or requirements have not been met.