Federal Aviation Administration

FAA SAFETY RISK MANAGEMENT GUIDANCE

Version 1.0
June 2024

This document is located on the Federal Aviation Administration (FAA) Safety Management Intranet site. The document was developed by the FAA Safety Management System (SMS) Committee and is owned and maintained by the Safety Management Division (AVP-300) within Aviation Safety (AVS).

FAA Safety Risk Management Guidance

Purpose

The purpose of this document is to provide guidance for identifying, managing, and conducting safety risk assessments on safety issues that cross multiple FAA Lines of Business (LOB)/Staff Offices when the organizations seek involvement from the FAA SMS Executive Council and/or the FAA SMS Committee. These cross-organizational safety risk assessments are conducted in accordance with FAA Order 8040.4, *Safety Risk Management Policy*.

Audience

This guidance applies to the following LOBs: Air Traffic Organization (ATO), Aviation Safety (AVS), Airports (ARP), Commercial Space Transportation (AST), and Security and Hazardous Materials Safety (ASH), as well as the Office of NextGen (ANG), which is a Staff Office. This guidance is broadly applicable to the National Airspace System (NAS), which would allow it to be applied to other FAA organizations in the future, if management determines broader application to be appropriate.

Scope

This guidance applies to all FAA organizations seeking FAA SMS Executive Council and/or FAA SMS Committee involvement in conducting cross-LOB safety risk assessments, in accordance with FAA Order 8040.4, *Safety Risk Management Policy*. This document may also be used by organizations that wish to conduct a safety risk assessment in accordance with FAA Order 8040.4 without the involvement of the FAA SMS Executive Council or the FAA SMS Committee.

Approval: PAULA F MARTINEZ

Digitally signed by PAULA F MARTINEZ
Date: 2024.06.11 13:14:59 -04'00'

FAA SMS Committee Chair

Change Management

Revision Number	Description of Change	Date
0.1	Draft Document	11/27/23
0.2	AVP-310 Comments Incorporated	01/23/24
0.3	AVSSMS Coordination Group and FAA SMS Committee Comments Incorporated	04/30/24
1.0	Original Document (Version 1.0)	06/04/24

Change Management Criteria

Full revisions of the FAA Safety Risk Management Guidance will be conducted by AVP-300 and reviewed by the AVSSMS Coordination Group and FAA SMS Committee. Administrative changes may be made by AVP-300 between full revisions. All revisions and changes will be documented in the above Change Management Table. Full revision versions will be denoted by a whole number (i.e., Version 1.0, 2.0, 3.0), and administrative change versions will be denoted by a decimal (i.e., Version 1.1, 1.2, 2.1).

Table of Contents

Introduction

The Federal Aviation Administration's (FAA) mission is to provide the safest, most efficient aerospace system in the world. In support of this mission, the FAA uses a Safety Management System (SMS) to integrate the management of safety risk into operations, acquisitions, rulemaking, and decision making. The SMS enhances the safety of the public and strengthens the FAA's worldwide leadership in aerospace safety.

The SMS consists of four components: Safety Policy, Safety Risk Management (SRM), Safety Assurance, and Safety Promotion. All four components work together to enable the FAA to manage safety within the National Airspace System (NAS); however, the focus of this document is SRM, with nuances of Safety Assurance throughout. SRM provides a formalized, proactive approach to system safety in which safety risk is identified, analyzed, assessed, and controlled to an acceptable level. The objective of SRM is to provide information regarding hazards, safety risk, and safety risk controls/mitigations to decision makers and to enhance the FAA's ability to address safety risk in the NAS. SRM consists of conducting a system analysis; identifying hazards; and analyzing, assessing, and controlling safety risk associated with the identified hazards. FAA Order 8040.4, *Safety Risk Management Policy*, describes standardized principles that enhance the FAA's ability to coordinate risk-based decision-making across organizations. Safety Assurance plays an important role in triggering SRM through the identification of potential hazards or ineffective safety risk controls, as well as its role in monitoring safety risk controls.

The FAA Lines of Business (LOBs)/Staff Offices have various systems in place for identifying and managing safety issues[1] within their respective domains. However, there are times when the scope or complexity of a potential safety issue may cross organizational boundaries and require linkages across those organizations to analyze and address potential safety issues/emerging risk, which may require elevating the issue to the FAA SMS Committee for decision and action. Many times, a cross-LOB SRM Team is established to conduct a safety risk assessment on the hazards related to the identified safety issue. When cross-LOB SRM Teams are established, they follow the FAA Order 8040.4 requirements and the guidance provided in this document to conduct the safety risk assessment and record the results in a Safety Risk Assessment Report and Safety Risk Assessment Report Addendum which provide critical information for safety risk decision making.[2]

The purpose of this document is to provide guidance for identifying, managing, and conducting safety risk assessments on safety issues that cross multiple FAA LOBs/Staff Offices when the organizations seek involvement from the FAA SMS Executive Council and/or the FAA SMS Committee. These cross-organizational safety risk assessments are conducted in accordance with the current version of FAA Order 8040.4. Please note that organizations often establish SRM Teams without engaging the FAA SMS Executive Council and/or the FAA SMS Committee. In these cases, the organizations' SRM processes are employed. Organization-specific SRM processes are consistent with, but may not be exactly the same as, the process described in the current version of FAA Order 8040.4.

[1] For the purposes of this document, the term "safety issues" encompasses both issues and planned changes. Safety issues and planned changes that are raised to the FAA SMS Committee for decision and action will go through the same processes. Any exceptions are indicated within this document.
[2] A cross-LOB SRM Team uses the definitions and risk matrices in FAA Order 8040.4 unless all stakeholder FAA organizations agree to use a different method or tool.

Specifically, this document describes:

- Methods and process for identifying and elevating safety issues;
- Planning cross-LOB safety risk assessments;
- Conducting the SRM process;
- Documenting cross-LOB safety risk assessments and obtaining mitigation approvals;
- A process for monitoring mitigation performance;
- A mechanism for escalating SRM-related concerns/disagreements;
- Hazard tracking and monitoring utilizing the Hazard Identification, Risk Management and Tracking (HIRMT) system;
- Roles and responsibilities for SRM stakeholders;[3]
- Templates for the cross-LOB SRM process;
- A list of SRM tools; and
- A list of SRM technical definitions for select terms.

For specific definitions of terms used in this guidance document, see Appendix B of FAA Order 8040.4.

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

Chapter 1. FAA Safety Issue Identification and Management Process

The Federal Aviation Administration (FAA) Safety Management System (SMS) Committee sponsored the effort to establish an FAA-level safety issue identification and management process that provides a corporate capability that works across the FAA Lines of Business (LOBs)/Staff Offices to:

- Strengthen the FAA's awareness of emerging risk before accidents or incidents occur by utilizing information sharing and collaboration across the FAA;
- Have a venue to regularly reassess previous analyses and related assumptions made to support past safety-related decisions; and
- Have an avenue to elevate safety issues[4] that may need additional evaluation or a broader review.

The FAA LOBs/Staff Offices have various systems in place for identifying and managing safety issues within their respective domains; however, there is a need to find linkages across those organizations to identify, highlight, and elevate potential safety issues/emerging risk to the appropriate management level for decision and action.

This chapter describes the process for identifying, highlighting, and elevating potential FAA-level safety issues/emerging risk to the appropriate management level for decision and action. Note that the term "FAA-level safety issues" refers to cross-LOB safety issues managed by the FAA SMS Committee.

1.1. Methods of Safety Issue Identification

There are two primary methods for identifying FAA safety issues that may need to be elevated to the FAA SMS Committee for management and tracking. The first is discovery of potential safety issues via the FAA LOB/Staff Office organizational processes. The second is identification of potential safety issues through the Issue Identification Function.

1.1.1. Potential Safety Issues Identified by FAA LOBs/Staff Offices

It is expected that FAA LOBs/Staff Offices have developed their own organization-specific criteria for identifying and elevating safety issues. In general, LOBs/Staff Offices should engage the FAA SMS Committee when an identified hazard's effects can be experienced in parts of the aerospace system that are in the purview of more than one LOB/Staff Office or when the controls for a hazard that resides in one LOB/Staff Office need to be implemented by more than one LOB/Staff Office.

FAA Order 8040.4, *Safety Risk Management Policy*, requires that a safety issue meeting one or more of the criteria listed below is considered an Aerospace System Level (ASL) safety issue and must be reported in and managed through the Hazard Identification, Risk Management & Tracking (HIRMT) system.

1. The safety issue is tracked and managed by the FAA SMS Committee;
2. The safety issue is present in the National Airspace System (NAS),[5] its safety risk has not been accepted, and it is expected to have high risk (e.g., it is identified as a result of

[4] For the purposes of this document, the term "safety issues" encompasses both issues and planned changes. Safety issues and planned changes that are raised to the FAA SMS Committee for decision and action will go through the same processes. Any exceptions are indicated within this document.
[5] Changes being processed through the NAS Change Proposal (NCP) may be considered to be present in the NAS if they are in the live test and evaluation phase.

an accident or incident, or it is assumed to have high risk, but an assessment has not been completed);
3. The safety issue has high risk and has a potentially systemic effect (e.g., the effect crosses LOBs or the effect impacts an industry segment rather than an individual certificate holder); or
4. Any safety issue that an FAA organization's management elects to track in HIRMT.[6]

In addition to ASL safety issues, the FAA SMS Committee may be interested in tracking or managing other safety issues in HIRMT. Examples include:

- The safety issue has medium or high risk associated with it according to the results of the preliminary safety risk assessment[7] conducted in accordance with the severity and likelihood definitions in FAA Order 8040.4.
- The safety issue is, or may reasonably become, highly visible or has the potential to be controversial with stakeholders.[8] Highly visible or potentially controversial safety issues could include safety issues that are the result of, or are related to, an accident or serious incident; safety issues that are considered high priority by FAA executives; and safety issues involving other federal organizations (e.g., based upon a National Transportation Safety Board [NTSB] recommendation or a Congressional report suggesting that a new control is necessary). Highly visible or potentially controversial safety issues may be currently in the news or have the potential for public sensitivity, and/or may have significant political, economic, or financial impact to the FAA, the NAS, or the public.

Additionally, an FAA organization's management may elect to track a safety issue in HIRMT because it requires management at the FAA level (i.e., FAA SMS Committee). The safety issue may need additional oversight and resources to address it and should be proposed for elevation to the FAA SMS Committee for the necessary support and visibility. In addition, LOBs/Staff Offices may identify other types of safety issues to be tracked in HIRMT.

LOBs/Staff Offices may use their own tools to collect and maintain information regarding safety issues that are addressed wholly within their organization; however, if the safety issue meets the ASL criteria, the information must be entered into HIRMT.

1.1.2. Potential Safety Issues Identified through Issue Identification Function

The Office of Accident Investigation and Prevention (AVP) manages the Issue Identification Function, which includes analysis of existing data, as well as utilization of subject matter expertise (including safety risk management and aerospace expertise). These two roles work together to anticipate possible future events and identify potential safety issues for consideration by the FAA SMS Committee.

As safety issues are assessed, the subject matter experts (SMEs) may consider, for example, whether:

- There is a trend of the safety issue (i.e., data indicating a negative trend);
- An FAA LOB/Staff Office or other entity has addressed or studied this safety issue previously, and if so, whether the result is still valid; and/or

[6] The organization should consider the risk and visibility of a safety issue when determining whether it should be entered into HIRMT.
[7] See Section 1.2.2, *Step 2: Conduct Preliminary Safety Risk Assessment*, for more information on preliminary safety risk assessments.
[8] A stakeholder is a group or individual that is affected by, or is in some way accountable for, the outcome of an undertaking; a stakeholder can also be described as an interested party having a right, share, or claim in a product or service or in its success in possessing qualities that meet that party's needs and/or expectations.

- There are gaps in a current FAA process that could lead to increased risk in the NAS.

Although the Issue Identification Function resides within AVP, AVP can request support from FAA LOBs/Staff Offices with expertise specific to the safety issue being studied.

The Issue Identification Function acquires, monitors, reviews, and assesses available information related to the aerospace system to identify potential safety issues in the system and determine whether the safety issues should be raised to the FAA SMS Committee. Examples of potential safety issues that may need to be considered by the FAA SMS Committee include, but are not limited to:

- Safety issues or potential hazards in the system identified through data analysis (e.g., analyses driven by Aviation Safety Information Analysis and Sharing [ASIAS]);
- Safety issues identified by industry or system users;
- Potential hazards or ineffective controls identified from the Safety Assurance and Mitigation Performance Monitoring (MPM) processes (see Chapter 5, *Mitigation Performance Monitoring Process*, for more information) that are considered potentially systemic and most effectively treated by cross-organizational or cross-LOB teams;
- Safety issues that are, or may reasonably become, highly visible, or have the potential to be controversial with stakeholders;
- Safety issues that could affect more than one FAA LOB/Staff Office, or if their mitigations require more than one FAA LOB/Staff Office to implement;
- New controls deemed necessary by the FAA as a result of internal FAA safety recommendations or recommendations from other external entities such as the NTSB, Congress, or Foreign Civil Aviation Authorities (FCAAs);
- Operational outlier events that expose latent safety risk;
- Safety issues that may arise from recommended or proposed aerospace system improvements, including new technologies; and
- Impending or urgent changes to the aerospace system causing existing safety risk controls to no longer be adequate.

Safety Assurance requires acquiring data and information from across the system to verify that risk analyses and mitigation actions are yielding the desired outcomes. As part of Safety Assurance, safety issues could be revisited with new information that may change original assumptions and/or decisions. AVP's intent is to leverage existing relationships and data from available information sources (e.g., ASIAS); however, AVP does not intend to duplicate or disrupt existing or ongoing work of other safety groups. Chapter 5, *Mitigation Performance Monitoring Process*, contains more detail on the Safety Assurance processes for cross-LOB safety issues.

AVP leverages the work from within its organization to identify safety issues which could potentially result in a systemic outcome or safety issues that are, or may reasonably become, highly visible or have the potential to be controversial with stakeholders. Examples of sources within AVP include outputs from the Accident Investigation Division daily briefings, ASIAS information, and NTSB and FAA safety recommendations.

AVP-300 meets periodically to review potential safety issues highlighted by the other AVP Divisions. In addition to the information found within AVP, other potential sources of information may include:

- Employee or stakeholder reporting systems;
- Congressional legislation or statutes;
- Inspections and mandatory reporting systems; and

- Other sources (e.g., Department of Transportation [DOT], Office of Inspector General [OIG], Office of Management and Budget [OMB], Government Accountability Office [GAO], news, newsletters).

1.2. Process for Identifying/Elevating Safety Issues

Figure 1-1 depicts the process flow for identifying and elevating FAA safety issues.

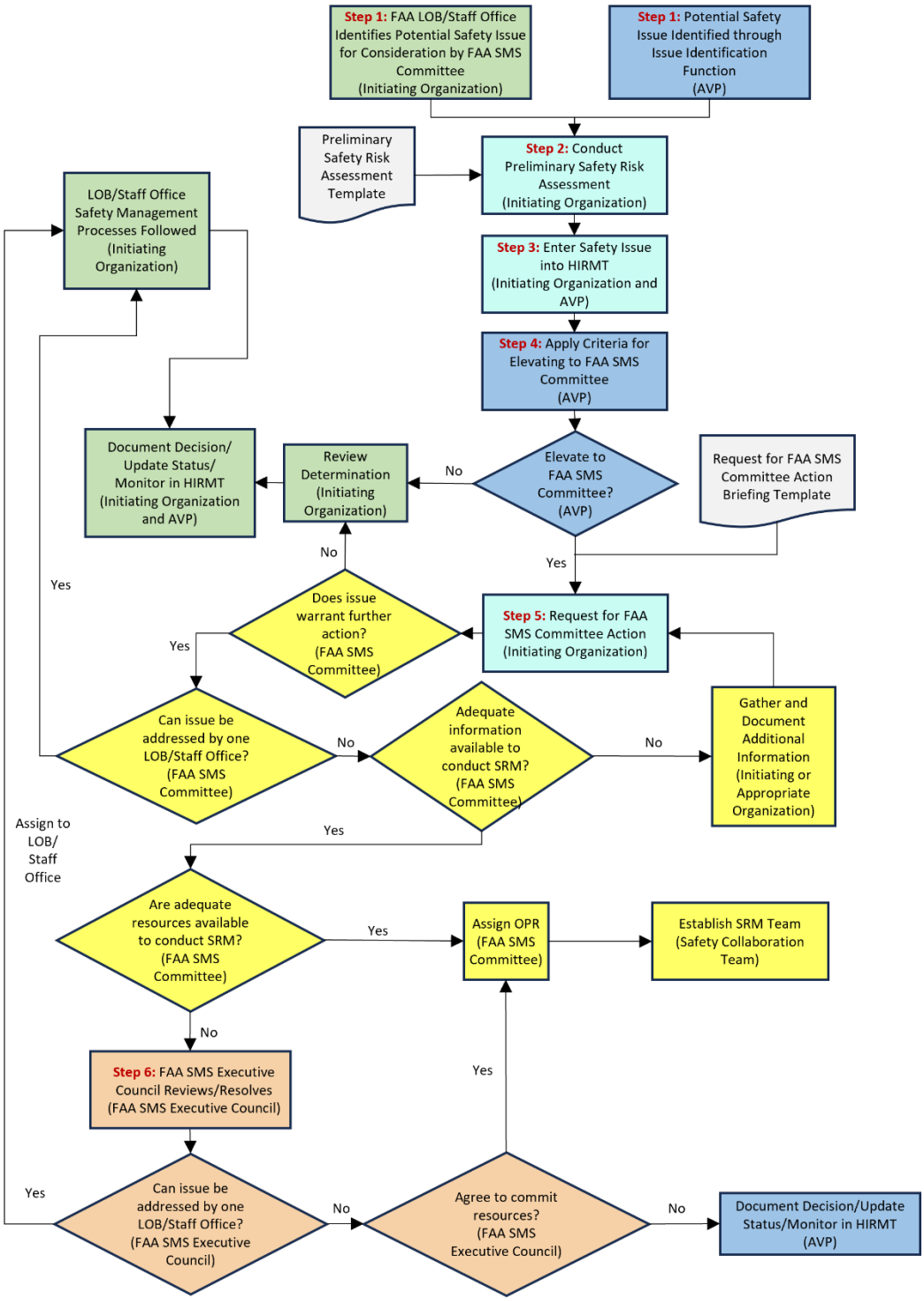


Figure 1-1: Process for Identifying/Elevating FAA Safety Issues

1.2.1. Step 1: Identify Potential Safety Issue

A potential safety issue for consideration by the FAA SMS Committee is identified either by an FAA LOB/Staff Office or through the Issue Identification Function within AVP. The organization that raised the safety issue is referred to as the Initiating Organization (see Appendix A, *Roles and Responsibilities*, for more information on this role). In this step, the Initiating Organization gathers all the known information regarding the safety issue, as well as any work that has been completed to address the safety issue.[9] Specifically, the safety issue information should include:

- Description of safety issue;
- List of stakeholders (internal and external to the FAA);
- Summary of safety assessments/analyses conducted to date[10] including:
    - A description of the tools or methods that were used to identify and analyze the safety issue, and
    - What group(s), if any, worked on or is currently working on the safety issue;
- Data/information that is available to support a safety assessment (e.g., accidents and/or incidents directly related to the safety issue); and
- Whether the safety issue is related to an active research and development (R&D) area.

1.2.2. Step 2: Conduct Preliminary Safety Risk Assessment

Once a safety issue has been identified, the Initiating Organization (or AVP for safety issues identified through the Issue Identification Function) conducts a preliminary safety risk assessment. If needed, AVP will work with the LOB/Staff Office to conduct the assessment. There is a Preliminary Safety Risk Assessment template available for Initiating Organizations to use. See Appendix B, *Templates*, for more information on the templates available.

Preliminary safety risk assessments need not be complex; the assessment's discussion of existing controls and potential hazards are intended to support decision makers in determining whether to direct resources toward a more detailed and complete analysis of the safety issue. Preliminary safety risk assessments are intended to be conducted with a small group of experts (possibly a single expert, depending on the safety issue) in a short amount of time.

1.2.3. Step 3: Enter Safety Issue in HIRMT

HIRMT is the FAA's official tool for collecting, managing, and reporting on ASL safety issues and those safety issues identified through this process, as well as the associated hazards and risk mitigations. Documentation from Steps 1 and 2 should be uploaded into HIRMT as supporting attachments to the HIRMT record. The Initiating Organization provides safety issue information necessary to populate the required fields in HIRMT and works with the HIRMT Program Manager within AVP-300 to have the information entered into HIRMT prior to elevating it to the FAA SMS Committee for decision or action.

Safety issues that are not selected for assessment with FAA SMS Committee involvement are still tracked and managed in HIRMT by AVP, and it is expected that the Initiating Organization would apply SRM processes to address the safety issue and provide periodic status updates to AVP so that HIRMT can be kept current.

[9] When gathering the necessary information, the Initiating Organization queries the Safety Collaboration Team (SCT) via their organization's FAA SMS Committee member (see the SMS Contacts page on the FAA Intranet for the list of members), as well as any other related groups.
[10] The Initiating Organization should search HIRMT for any existing related issues in addition to any other activities related to the safety issue.

At this stage, a representative from the Initiating Organization should request access to HIRMT. While the HIRMT Program Manager enters safety issue information, access to HIRMT will allow the Initiating Organization to check the status and report on the progress of the safety issue. See Chapter 7, *Hazard Identification, Risk Management and Tracking (HIRMT) System*, for additional information regarding accessing HIRMT.

1.2.4. Step 4: Apply Criteria for Elevating to FAA SMS Committee

In this step, AVP (acting on behalf of the FAA SMS Committee) works with the Initiating Organization to apply criteria to the safety issue to determine whether the safety issue should be elevated to the FAA SMS Committee. The Initiating Organization should deliver all information related to the safety issue, including the Preliminary Safety Risk Assessment, to the Safety Risk Management and Safety Assurance Branch (AVP-310) for review. AVP-310 will review the information for accuracy and completion, as well as assist the Initiating Organization in applying the elevation criteria listed below. If there are any changes made to the Preliminary Safety Risk Assessment, the Initiating Organization or Office of Primary Responsibility (OPR) should work with the HIRMT Program Manager to upload the updated version into HIRMT. While the primary focus is on prioritizing resources to address the highest safety risk in the system, the process allows managers to increase visibility of safety issues that meet other criteria. If the safety issue meets any of the following criteria, it is elevated to the FAA SMS Committee for action (see Section 1.2.5, *Step 5: Request for FAA SMS Committee Action*).

Medium or High Risk Identified

The safety issue has medium or high risk associated with it according to the results of the Preliminary Safety Risk Assessment conducted in accordance with the severity and likelihood definitions in FAA Order 8040.4.

Potential Systemic Outcome

The safety issue has the potential to result in a systemic (system-wide) outcome. A safety issue with a potentially systemic outcome affects multiple FAA LOBs/Staff Offices or multiple segments of industry rather than an individual certificate holder. Also considered are the number of components/system segments involved; the number of Code of Federal Regulations (CFR) parts involved; and whether the safety issue potentially has national, regional, or local impact.

Highly Visible or Potentially Controversial

The safety issue is or may reasonably become highly visible or has the potential to be controversial with stakeholders. Highly visible or potentially controversial safety issues could include safety issues that are the result of, or are related to, an accident or serious incident; safety issues that are considered high priority by FAA executives; and safety issues involving other federal organizations (e.g., based upon an NTSB recommendation or a Congressional report suggesting that a new control is necessary). Highly visible or potentially controversial safety issues may be currently in the news or have the potential for public sensitivity, and/or may have significant political, economic, or financial impact to the FAA, the NAS, or the public.

Management Discretion

The safety issue is deemed by FAA management (Director-level or above) to require management at the FAA-level. The safety issue may need additional oversight and resources to address it and is proposed for elevation to the FAA SMS Committee for the necessary support and visibility.

1.2.5. Step 5: Request for FAA SMS Committee Action

In this step, AVP-310 works with the Initiating Organization to formally request action or decision from the FAA SMS Committee. The Initiating Organization should work with AVP-310 to obtain approval of the briefing to the FAA SMS Committee (see Appendix B, *Templates*), which should include:

- Description of safety issue;
- List of stakeholders (internal and external to FAA);
- Summary of safety assessments/analyses conducted to date including:
    - A description of the tools or methods that were used to identify and analyze the safety issue,
    - What group(s), if any, worked on or is currently working on the safety issue, and
    - Data/information that is available to support a safety assessment (e.g., accidents and/or incidents directly related to the safety issue);
- Results of the Preliminary Safety Risk Assessment (including preliminary hazards) and assessment of impact of the safety issue/change on the aerospace system; and
- Requested action/decision from the FAA SMS Committee.

The FAA SMS Committee can decide to:

- Refer the safety issue back to the Initiating (or Appropriate) Organization because the safety issue does not warrant further action by the FAA SMS Committee;
- Send the safety issue to an LOB/Staff Office to address (assign as OPR) and monitor in HIRMT;
- Gather and document additional information/data from an appropriate organization and/or conduct further data analysis;
- Establish an SRM Team; or
- Elevate the safety issue to the FAA Executive Council.

The FAA SMS Committee may decide that the safety issue does not warrant further study at the FAA level. For instance, the FAA SMS Committee may determine that resources should be spent on a higher priority safety issue, or that another safety team is adequately addressing the safety issue. In these cases, the safety issue is routed back to the Initiating (or Appropriate) Organization to document the decision and justification and work with AVP to update the safety issue status in HIRMT.

If the FAA SMS Committee decides the safety issue can be addressed within an LOB/Staff Office, the FAA SMS Committee assigns an OPR and directs the OPR to document and track the safety issue in HIRMT.

If the FAA SMS Committee decides that additional data or further data analysis is needed, it will typically send a request to the appropriate organization to gather and document additional information/data and/or examine the safety issue in more depth and report the findings to the FAA SMS Committee for reconsideration of the safety issue.

If the FAA SMS Committee determines the need for a safety risk assessment of a safety issue, the Committee, with assistance from the Initiating Organization, identifies the OPR. In general, the candidate OPR would typically be the organization that has the largest stake in the safety issue or change and/or is in the best position to address the safety issue.[11] The FAA SMS

[11] The OPR for a rulemaking project will generally be the OPR for the Safety Risk Assessment as well.

Committee Chair may delegate the initial OPR request to the appropriate manager in the Initiating Organization, Safety Collaboration Team (SCT) Leadership, or another member of the FAA SMS Committee. See Appendix A, *Roles and Responsibilities*, for more information regarding the roles and responsibilities of the OPR.

The FAA SMS Committee also tasks the SCT to manage the safety risk assessments of FAA-level cross-LOB safety issues. SCT Leadership reaches out to the OPR Point of Contact (POC) to offer assistance with the SRM process. Cross-LOB SRM Teams follow the requirements in the current version of FAA Order 8040.4, as well as the guidance in Chapters 2, 3, and 4 of this document.

Typically, prioritization of safety issues and identification of necessary resources are handled by the FAA SMS Committee. However, the FAA SMS Committee can elevate safety issues to the FAA SMS Executive Council if the necessary resources are not available, or if a conflict needs to be resolved (see Section 1.2.6, *Step 6: FAA SMS Executive Council Reviews/Resolves*). The FAA SMS Committee Chair will provide status updates on safety issues managed through this process at the regularly scheduled FAA SMS Executive Council meetings for all safety issues that are elevated to the FAA SMS Committee. The FAA SMS Committee members ensure that the LOBs/Staff Offices involved provide appropriate SMEs needed for the discussions at the FAA SMS Executive Council meetings.

If an organization disagrees with the FAA SMS Committee decision, the organization should submit a request to the FAA SMS Committee Chair either for reconsideration by the FAA SMS Committee or escalation to the FAA SMS Executive Council.

1.2.6. Step 6: FAA SMS Executive Council Reviews/Resolves

If the FAA SMS Committee finds that a resolution on the safety issue cannot be reached or additional resources are required, the FAA SMS Committee Chair raises the unresolved safety issue to the FAA SMS Executive Council for resolution. Depending on the urgency of the safety issue, this can be done at a regularly scheduled FAA SMS Executive Council meeting or at a special meeting called to discuss the safety issue.

The FAA SMS Committee members ensure that the LOBs/Staff Offices involved provide appropriate SMEs needed for the discussions at the FAA SMS Executive Council meeting. The FAA SMS Committee Chair communicates the results of the FAA SMS Executive Council meeting with the FAA SMS Committee members and OPR, who in turn share the information with their organizations.

The FAA SMS Executive Council can decide to:

- Send the safety issue back to the LOB/Staff Office to monitor in HIRMT;
- Commit additional resources and send the safety issue back to the FAA SMS Committee to:
    - Request an appropriate organization to gather and document additional information/data, and/or conduct further data analysis, or
    - Establish an SRM Team;
- Not commit any additional resources, in which case the decision and status are documented in HIRMT; or
- Agree with either the FAA SMS Committee, or the organization, for FAA SMS Committee decisions that have been requested for reconsideration.

The decision made by the FAA SMS Executive Council will be documented in HIRMT.

Chapter 2. Planning Cross-LOB Safety Risk Assessments

All cross-LOB SRM Teams established by the FAA SMS Committee via the FAA Safety Issue Identification and Management Process described in Chapter 1 and organized by the SCT will follow the process in Chapters 2, 3, and 4. This chapter describes the activities involved in planning cross-LOB safety risk assessments.

Figure 2-1 depicts the activities and templates involved in planning cross-LOB safety risk assessments.

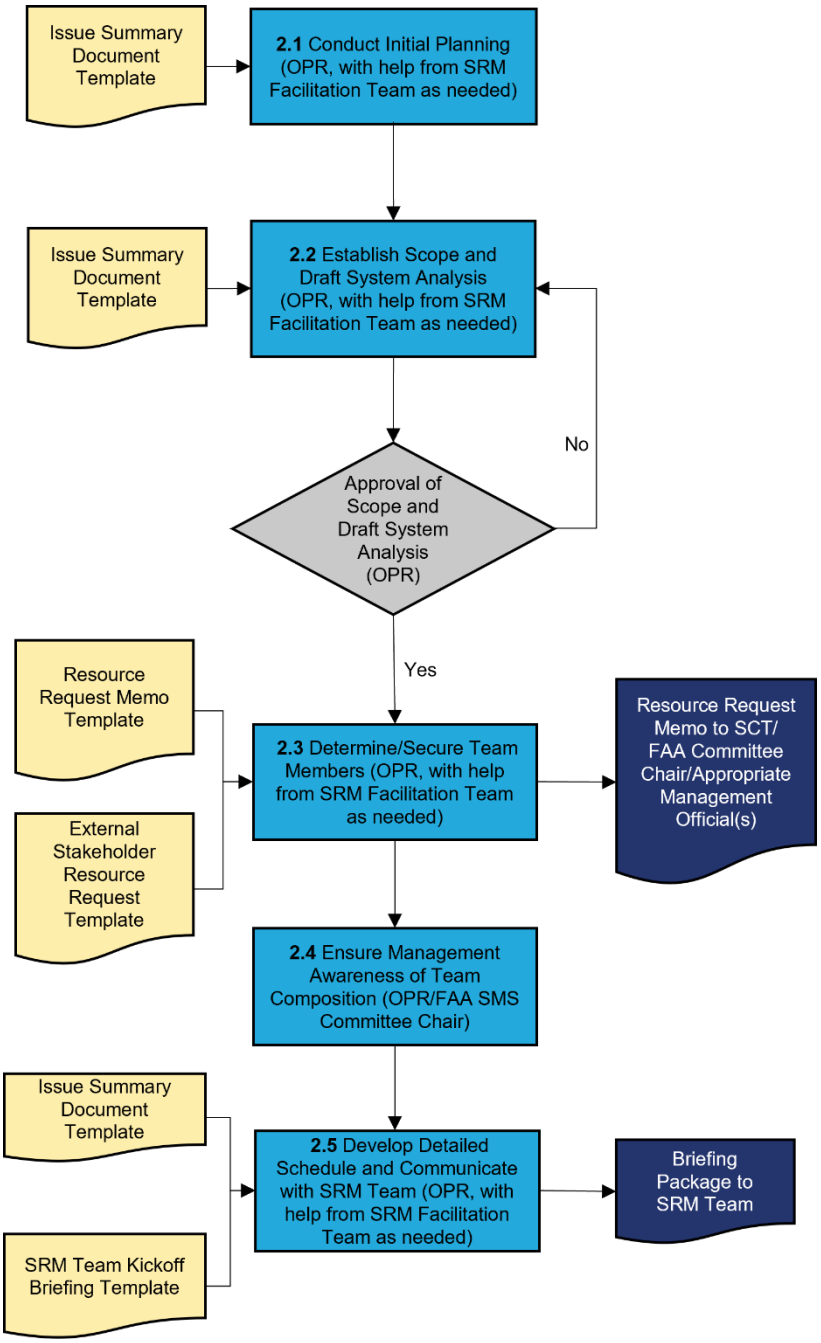


Figure 2-1: Planning Cross-LOB Safety Risk Assessments

2.1. Conduct Initial Planning

Initial planning for a cross-LOB safety risk assessment can begin once the FAA SMS Committee or Executive Council has approved the establishment of an SRM Team, an OPR has been identified, and the safety issue has been entered into HIRMT, per the FAA Safety Issue Identification and Management Process described in Chapter 1. Initial planning is necessary to document the goals and objectives of the SRM Team and define a timeline for the assessment so that a high-level plan can be communicated to stakeholders.

In this step, the OPR POC, with assistance from the SCT, identifies the SRM Facilitation Team, which typically includes SRM Facilitator(s) and a Documentation Analyst. The OPR POC and SRM Facilitation Team may also decide to include a data SME during the initial planning to ensure access and analysis to data needed for the assessment. Then, the OPR POC (with assistance from the SRM Facilitation Team, as needed) documents a brief description of the safety issue, describes the preliminary scope of the assessment, and identifies stakeholders and participating organizations. The OPR POC and Facilitation Team develop a schedule that includes high-level milestones for planning, conducting, documenting, and obtaining approvals for the safety risk assessment; they use the Issue Summary Template (see Appendix B, *Templates*) to document this information. The template is used as a summary outreach document when requesting participation on the SRM Team.

2.2. Establish Scope and Draft System Analysis

The OPR POC and SRM Facilitation Team (with assistance from the SCT, as needed) continues to document the draft scope of the assessment, Team composition, and the system analysis in the Issue Summary Template. The OPR POC (with participation from the SCT, as needed) meets with the SRM Team Facilitator(s) to plan the SRM Team meetings. Preparation meetings are used to define:

- The proposed safety issue;
- The draft system state(s) in which the safety issue is or will be operational;
- Assumptions (not existing controls) that may influence the analysis;
- The components of the 5M Model;[12]
- Sources of relevant data/information related to the safety issue; and
- Appropriate method and applicable risk matrix for the safety risk assessment (according to FAA Order 8040.4).

The purpose of the system analysis step is to understand and describe the system to the extent necessary to identify potential hazards. It is a comprehensive approach to examining a safety issue in terms of what it affects and what is affected by the safety issue. The OPR POC typically uses the 5M Model[12] to capture the information needed to bound and describe the system and aid in the hazard identification process. When defining the components of the 5M Model (see Issue Summary Template), the OPR adheres to the following guidelines:

- **Mission:** Define the safety issue being assessed. There should be agreement on the language for the safety issue that the SRM Team is tasked to assess. Ensure that the language is unambiguous, concise, and clearly reflective of the safety issue or change.
- **(hu)Man:** Define the human operators, maintainers, and affected stakeholders. Identify organizations and groups that are affected by the safety issue. Stakeholders include

[12] The OPR may decide to utilize a different tool to draft the system analysis. See Appendix C, *SRM Tools*, for other tools.

those exposed to harm/damage and those responsible for safety risk controls and may also include both internal and external organizations.

- **Machine:** Define the equipment used in the system that is related to the safety issue, including, but not limited to, hardware, firmware, software, human-to-system interfaces, system-to-system interfaces, and avionics.
- **Management:** Define the documents that are relevant to the safety issue (e.g., directives, policies, Standard Operating Procedures [SOPs], Letters of Agreement).
- **Media:** Define the environment in which the system is operated and maintained (i.e., the elements of the NAS that are affected by the safety issue).

The information included in the 5M Model will be reviewed and likely edited by the SRM Team during the SRM Team Kickoff meeting to reach agreement among the SRM Team members.

At this point, the OPR POC and SRM Team Facilitator(s) may choose to define the Team's risk assessment methodology. FAA Order 8040.4 allows flexibility to account for existing LOB/Staff Office processes and structure. If another methodology would be more appropriate for the assessment, the OPR can work with the other stakeholder FAA organizations to come to an agreement on the risk assessment criteria that will be used for the assessment. The OPR POC and SRM Facilitator(s) should then document the risk assessment criteria in the 5M Model in the Issue Summary Template.

After the assessment scope and draft system analysis are complete, the OPR POC forwards them to the OPR Manager for review and approval, as applicable. The OPR documents that the assessment scope and draft system analysis are complete by coordinating with the HIRMT Program Manager to have the completed templates uploaded to the safety issue record in HIRMT, noting the OPR Manager's approval.

Once the OPR Manager's acceptance is obtained, the OPR POC and SRM Team Facilitator(s) coordinate to develop a briefing package to provide to the SRM Team members.

2.3. Determine and Secure SRM Team Members

SRM Teams should include representatives from the various organizations affected by the safety issue. It is important that the Team be diverse and include stakeholders and experts who are expected to be involved in various capacities throughout the SRM process, while maintaining the right number of participants to ensure the Team can be efficiently managed. Team members should be given authority by their management to speak on behalf of their organization.

SRM Teams should always strive for consensus. However, in some cases, the SRM Team may need to put some decisions to a vote.[13] Prior to the SRM Team meeting, the OPR and Facilitation Team should decide which level of organization should receive one vote (i.e., branch level, organization level, LOB level) based on the structure of the SRM Team. While an organization may send multiple people, only one Team member should be given authority to vote on behalf of the organization.

[13] SRM Team members may vote on risk levels, proposed safety recommendations, and the Monitoring Plan. However, the SRM Team will not make decisions on which proposed safety recommendations will be implemented; FAA management will make the final determination on which to implement.

There are two distinct roles within an SRM Team that the OPR and Facilitation Team should consider when requesting resources—SRM Team Members and Observers. The two roles are briefly described below. For more information on all roles within the SRM Process, see Appendix A, *Roles and Responsibilities*.

- **SRM Team Member:** An FAA employee or approved external stakeholder who is knowledgeable of and/or directly affected by the safety issue being assessed. The role includes, but is not limited to the following duties:
    - As a Team, conducts SRM on the issue in accordance with FAA Order 8040.4C.
    - Objectively examines and assesses potential safety risk of the issue or change and associated hazard(s).
    - Reviews the Team's safety findings, as documented by the Documentation Analyst, in a Safety Risk Assessment Report.
- **SRM Team Observer:** An FAA employee, approved external stakeholder, or data expert, or an individual who is seeking to gain additional knowledge on the safety issue being assessed and/or the SRM process. The role includes the following specifications:
    - Attends meetings but does not participate in SRM Team discussions or decisions unless specifically called upon by the SRM Team to contribute.
    - Does not participate in Safety Risk Assessment Report or Addendum reviews or provide comments.

As discussed further below, there are safety issues for which the FAA may request participation from non-governmental entities or governmental entities outside of the FAA. Depending on the situation, OPRs should reach out to the Office of the Chief Counsel (AGC) for confirmation on which role external participants should perform on the SRM Team. When determining the composition of the SRM Team, OPRs should consider the balance of interest—that is, the organizations accepting or mitigating risk should be more likely to be SRM Team members (i.e., have a vote in the assessment).

The OPR POC (with assistance from the SRM Facilitation Team and/or SCT, if needed) identifies the skills and expertise required to conduct the safety risk assessment.[14] Though the size and makeup of the cross-LOB SRM Team varies according to the type and complexity of the safety issue, the following types of experts should be considered for involvement on the Team (note that this list is not all-inclusive):

- Employees directly responsible for the safety issue being analyzed/assessed;
- Employees with current knowledge of and experience or operational proficiency with the safety issue;
- Hardware or software engineering or automation experts to provide knowledge on equipment performance;
- Air traffic controllers and pilots;
- Human factors specialist;
- Medical specialist;
- Quality Assurance expert to help ensure the safety performance measures are auditable/measurable; and
- Employees skilled in collecting and analyzing hazard and error data and using specialized tools and techniques (e.g., operations research, data, human factors, failure mode analysis).

[14] If requesting participation from bargaining unit members, follow the SOP for Requesting Bargaining Unit/SME Support and Program Overtime.

As stated previously, in order to conduct a thorough assessment, it is important to have all necessary expertise on the SRM Team. At times, this means that the FAA might request participation from entities outside the agency, including product/service provider organizations for which the FAA has oversight responsibility. In such cases, the OPR must confer with the AGC to follow any data protection and Freedom of Information Act (FOIA) requirements, and/or avoid any potential legal/statutory issues. This is especially advisable if the SRM Team will have access to data/information that is not publicly available. Note that coordinating participation from external stakeholders may require additional time and documentation.

To ensure the quality of participation from Team members, it is important that all Team members have a basic understanding of SRM prior to commencing the SRM Team meetings. All FAA SRM Team members should review the FAA SRM Overview Briefing (FAA27000023) in the electronic Learning Management System (eLMS) prior to participating on an SRM Team. A similar overview should be provided to any external Team participants. The Kickoff Meeting (discussed in Section 2.5, *Develop Detailed Schedule and Communicate with SRM Team*) is an opportunity to provide all SRM Team members (external participants included) with an overview of the SRM process.

The OPR POC determines the expectations of Team members regarding the level of effort required to support the Team. Expectations include:

- **Face-to-face or videoconference meetings:** Estimate how many meetings the SRM Team is expected to attend in person or online, the location(s) of the meetings (if in person), and the duration of the meetings required to accomplish the Team objectives.
- **Teleconferences:** Estimate the frequency of expected teleconferences, duration of the calls, and timeframe they are expected to occur (e.g., every two weeks for 1 hour, June–October). Specify the time zone in which the calls will take place.
- **Work outside of meetings:** Estimate the type (e.g., collection of data) and amount of work that the Team member will be expected to complete in between the meetings and teleconferences (e.g., it is anticipated that the Team member will spend 10 hours per week devoted to this activity outside of the face-to-face/videoconference meetings and teleconferences).

In addition to expectations about the level of effort, the OPR POC identifies any other factors that organizations should consider when selecting Team members and specific participant roles, which include:

- The Team member’s ability to represent their organization’s perspective;
- The Team member’s objectivity sufficient to consider safety risk outside of their LOB/Staff Office;
- The Team member’s ability to consider safety risk at an LOB/Staff Office level and system level;
- The impact on the organization of a Team member being away from normal duties;
- The Team member’s ability to interface with other organizations; and
- The balance of personality traits of all Team members.

Next, the OPR POC reaches out to existing contacts within FAA organizations (e.g., AVSSMS Coordination Group, FAA SMS Committee), provides the contacts with an overview of the project, and requests recommendations for people who might be a good fit for the Team. The outcome of this coordination is a list of possible candidates for each Team member position.

The formal participation request for SRM Team members is made using the Resource Request Memo Template (see Appendix B, *Templates*). The OPR POC and SRM Team Facilitator work

with the SCT Co-Chairs to complete the memo, which the FAA SMS Committee Chairperson and AVSSMS Coordination Group Chairperson distribute to managers of all requested Team member organizations. The External Stakeholder Resource Request Template (see Appendix B, *Templates*) is used to request participation from SMEs outside the FAA. As mentioned previously, when non-governmental entities are invited to participate on SRM Teams, the OPR must confer with AGC to avoid potential data protection and/or legal statutory issues, as well as comply with FOIA requirements. When governmental entities outside of the FAA are invited, OPRs should confer with AGC. OPRs are encouraged to meet with the other governmental entities before the SRM Team convenes to introduce the process and understand any sensitive topics that should not be discussed with non-governmental entities.

The OPR POC and Facilitation Team then revise the Issue Summary with the names and contact information of requested SRM Team members. The OPR works with the HIRMT Program Manager to upload the completed Issue Summary into HIRMT for documentation purposes.

2.4. Ensure Management Awareness of Team Membership

It is important to ensure that LOB/Staff Office leadership is aware of who in the organization is participating in the safety risk assessment. For FAA-level safety issues, the FAA SMS Committee Chair may present high-level milestones, an associated schedule, and the SRM Team composition, in the form of an abbreviated Issue Summary, to the FAA SMS Executive Council for awareness.

2.5. Develop Detailed Schedule and Communicate with SRM Team

Once the SRM Team members are secured, the OPR POC (with assistance from the SRM Team Facilitator) develops a more detailed schedule and adds it to the existing Issue Summary.

The OPR POC and the Facilitation Team meet to prepare and develop a briefing package for the SRM Team Kickoff Meeting. The purpose of the kickoff meeting is to introduce the safety issue to the Team, provide an overview of the SRM process, and determine whether any additional information or data should be gathered prior to the SRM Team meeting. The kickoff meeting should be scheduled two weeks prior to the SRM Team meeting, if possible. The briefing package for the SRM Team kickoff meeting includes:

- An agenda for the meeting;
- A briefing (see more information on the SRM Team Kickoff Briefing Template in Appendix B, *Templates*), which includes:
    - A summary of the goals and objectives for the SRM Team,
    - A summary of the safety issue,
    - An overview of the FAA SRM Process,
    - SRM Team ground rules, and
    - The assessment method(s) by which the SRM Team will identify hazards;
- The Issue Summary, containing a draft of the system analysis and a description of the safety issue; and
- The SRM Team Roles and Responsibilities information sheet.

The SRM Team Facilitator provides the briefing package, in addition to the meeting invitation and directions to the meeting or videoconference information, to the SRM Team sufficiently in advance of the initial meeting. The SRM Team Facilitator advises SRM Team members to review the briefing package and members that are FAA employees/contractors to complete the FAA SRM Overview in eLMS (FAA27000023).

Chapter 3. Conducting the SRM Process

The SRM Team, guided by the Facilitation Team, conducts the safety risk assessment in accordance with the current version of FAA Order 8040.4 by following the 5-Step SRM Process. Typically, the SRM Team completes all five SRM steps while convened together for a few days to conduct the safety risk assessment. However, there are times when SRM Teams reconvene if additional data, information, or analysis is necessary. The SRM Team typically conducts the assessment using the Hazard Analysis Worksheet (HAW) Template (see Appendix B, *Templates*). Alternative or additional SRM tools that can be used are described in Appendix C, *SRM Tools*.

3.1. SRM Process Overview

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. According to FAA Order 8040.4, a hazard is a condition or an object with the potential to cause or contribute to an incident or aircraft accident, as defined in 49 CFR § 830.2. Hazards are conditions that affect operations in a way that could result in degraded system performance and ultimately may result 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 3-1, the 5-Step SRM process is continuous, meaning that steps are repeated until the safety risk associated with each hazard is acceptable.

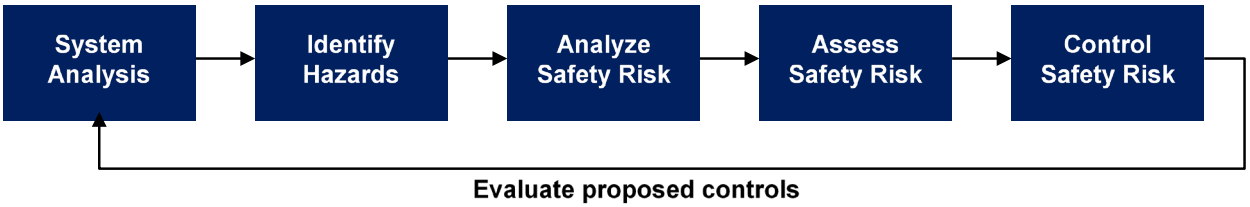


Figure 3-1: 5-Step SRM Process

3.2. Acceptable Data for Use in SRM

As explained in FAA Order 8040.4, acceptable data for use in SRM can be roughly classified into three categories: analytical, empirical, and judgmental. Analytical data is quantitative and based on analysis or logic. It typically has the lowest margin of error of the three types. Empirical data is also quantitative but is based on measurements from observed or simulated effects. The margin of error for empirical data can be controlled by sample size. Judgmental data is qualitative and based on expert opinion. It has the largest margin of error due to human biases and subjective experiences.

While any data is better than no data, when available, analytical data is preferred, followed by empirical, and finally judgmental. Analytical and empirical data can provide a solid calculation of overall safety risk, where judgmental data can ground the data to real-world situations. Analytical or empirical data tend to provide more objective results; however, when quantitative data is not available, it can be acceptable to rely on judgmental data. For example, to forecast the future, some amount of judgmental data may be required in addition to analytical or empirical data. 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, decision makers can consider the result of judgmental data.

Characteristics of quantitative data (analytical and empirical data) include:

- Data are expressed as quantities, numbers, or amounts.
- Data tend to be more objective, if underlying assumptions are correct.
- Data allow for more rational analysis and substantiation of findings.

Characteristics of qualitative data (judgmental data) include:

- Data are expressed as measures of quality.
- Data are subjective, but still grounded in experience and observation.
- Data allow for examination of subjects that can often not be expressed with numbers but by expert judgment.

Modeling techniques permit all three types of data as inputs (see Appendix C, *SRM Tools*, for more information on modeling techniques). If modeling is required and analytical or empirical data are available, the safety risk assessment should be based on that data. Where there is insufficient data to construct purely statistical or observational assessments of safety risk, judgmental data can be used.

Regardless of the data type(s) used, a thorough rationale for the choice must be articulated in the final Safety Risk Assessment Report.

3.3. Facilitation and Consensus Building

The SRM Team Facilitator mediates and assists SRM Team members in working through differences of opinion. The Facilitator should be able to remain neutral during these discussions, and recognize, acknowledge, and use differences of opinion to help the SRM Team consider different points of view. The SRM Team should strive to reach consensus, but in some cases, the SRM Team may need to put decisions to a vote.[15] While an organization may send multiple people, only one Team member should be given authority to vote on behalf of the organization. Should a vote take place, the results of the vote should be documented in the Safety Risk Assessment Report. There may be instances in which SRM Team members wish to submit their opinions in writing, including dissenting opinions. In those cases, the Team documents the results of the assessment, records the comments and other opinions, and delivers the results to the decision maker. Records of comments and other opinions are appended to the Safety Risk Assessment Report, if necessary, using the Record of Comments and Other Opinions Template (see Appendix B, *Templates*). If there is a concern or disagreement that should be raised to the FAA SMS Committee for resolution, the OPR should use the process in Chapter 6, *Escalation of SRM-Related Concerns or Disagreements*.

3.4. Step 1: System Analysis

3.4.1. Overview

As part of the safety risk assessment, the SRM Team must create a detailed description of the system in which the safety issue needs to be assessed. A complete and accurate system description is a critical foundation for conducting a thorough, unbiased safety analysis. The

[15] SRM Team members may vote on risk levels, proposed safety recommendations, and the Monitoring Plan. However, the SRM Team will not make decisions on which proposed safety recommendations will be implemented; FAA management will make the final determination on which to implement.

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 SRM planning.
- Work with data SMEs to gather the relevant available data/information regarding the safety issue to be analyzed. This includes available incident/accident data; information about the scope of exposure; previous applicable analyses and assessments; and related requirements, rules, and regulations, as necessary.
- 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 one system could affect the interfaces with other 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 (physical conditions, weather, etc.)
- 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 (means to reduce or eliminate the effects of hazards)

3.4.2. Scope of System Analysis

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 safety risk assessment. A complete and accurate system description is

the foundation for conducting a thorough safety analysis. System descriptions need to exhibit three essential characteristics—correctness, completeness, and clarity.

- 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.
- Clarity means that the system description is clear and understandable to all readers, including decision makers who may not be experts in all details of the safety issue.

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, complete, and clear. 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 interconnectivities and/or interdependencies between systems?
    - Does the system provide source material as input to external 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 safety issue impact system users?
- What existing risk controls are present in the system or change? What feedback is expected to ensure the controls are working appropriately?

The following are examples of data that the SRM Team could consider when describing the system.

- Number of flight hours affected by the safety issue
- Average annual approaches to each runway
- Number of hours the airport is at or below minimums
- Number and type of airport operations
- Number of landings and takeoffs, Instrument Flight Rules (IFR) and Visual Flight Rules (VFR) operations, and transitions
- Number of hours the airport is in visual meteorological conditions (VMC) vs. instrument meteorological conditions (IMC)
- 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 vehicle/pedestrian deviations
- Accident/injury data

3.4.3. 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. Appendix C, *SRM Tools*, contains additional information regarding system description and analysis models.

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

3.4.4. 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 safety issue.

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

When determining both depth and breadth of the safety analysis, the SRM Team should consider how much information is required to know enough about the safety issue, the associated hazards that will be identified during the assessment (see Section 3.5, *Step 2: Identify Hazards*), and each hazard's associated safety 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 risk level. The role of the SRM Team is to objectively identify and 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.
- 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 safety issue. 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.

3.5. Step 2: Identify Hazards

3.5.1. Overview

Once the system has been completely and accurately described (see Section 3.4, *Step 1: System Analysis*), the SRM Team identifies hazards. A hazard is a condition or an object with the potential to cause or contribute to an incident or aircraft accident, as defined in 49 CFR § 830.2. 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 safety issue 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.

3.5.2. Elements of Hazard Identification

The SRM Team needs the following, at a minimum, to identify hazards:

- Operational expertise
- Training or practical experience in various hazard analysis techniques
- A defined hazard analysis tool
- System description as outlined in Step 1, System Analysis

The SRM Team must also identify data sources and measures, which are necessary to identify hazards. The SRM Team selects the tool that is most appropriate for the type of system being evaluated. Appendix C, *SRM Tools*, contains tools/methods used for identifying hazards.

3.5.3. Potential Sources of Hazards

The SRM Team considers all 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 provide sources for hazards. Standardized hazard taxonomies are another potential resource for hazard identification. More information on potential sources of hazards is included in Section 3.8.5, *Defenses in Depth*. For guidance on SRM of systems in FAA acquisitions, please refer to the SRM Guidance for System Acquisitions (SRMGSA).

3.5.4. Causes, System States, and Effects

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 consider all system states. 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** – IMC vs. VMC, peak vs. low traffic, etc.
- **Physical** – Electromagnetic environmental 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 safety 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. SRM Teams should be cautious not to unnecessarily partition hazards (e.g., those with similar causes, controls, effects) which could have the unintended consequence of producing multiple lower risk hazards versus few higher risk hazards.

The SRM Team should also address the cumulative effect 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 the real outcome that has occurred, or a potential outcome with a probability of occurring that is greater than or equal to 1×10^{-11}, if the hazard exists in the defined system state.

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

3.5.5. 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 safety risk controls. The hazard model shown in Figure 3-2 was developed to ensure that the necessary components for the safety risk analysis are understood and identified while applying the SRM process.

According to FAA Order 8040.4, a hazard is a condition or object with the potential to cause or contribute to an incident or aircraft accident, as defined in 49 CFR § 830.2. Hazard identification must consider all reasonable possibilities, from the least to the most likely. The hazards to be included in the final analysis must be reasonable hazards considering all applicable existing controls. If the probability of a hazard's effect is less than 1×10^{-11}, it does not need to be considered in the assessment.

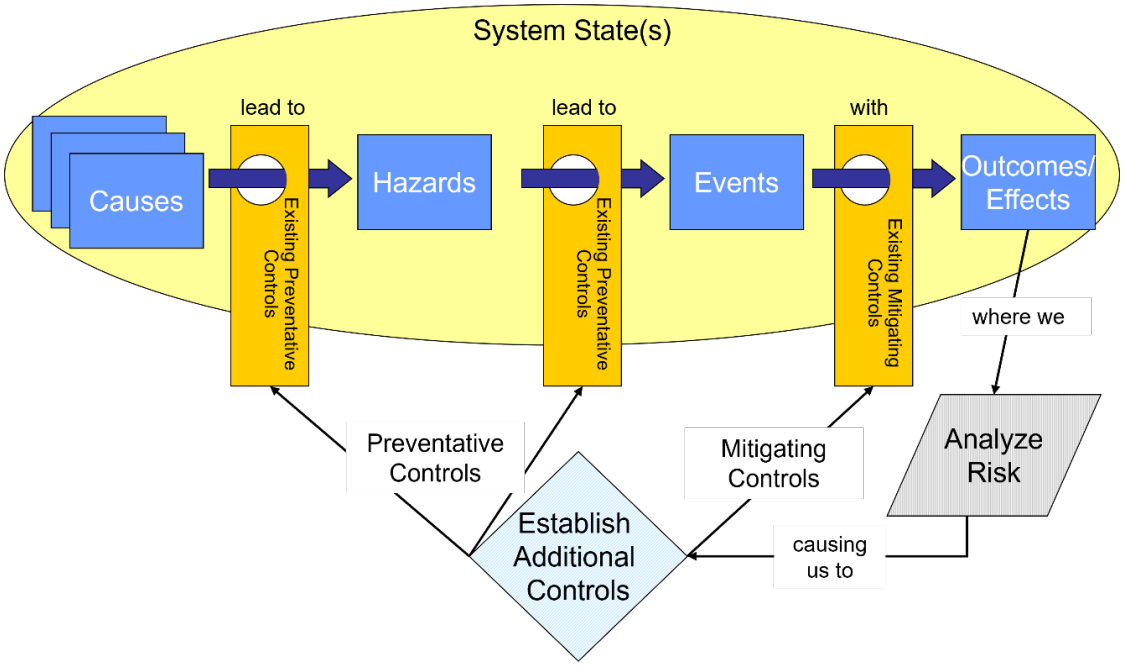


Figure 3-2: Hazard Model

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 safety issue and development of safety risk controls if necessary. However, each cause of a hazard may have its own cause. For example, the hazard “loss of situational awareness” could be caused by pilot distraction, complacency, fatigue, etc., each of which may have their own causes. In addition, causes and hazards are affected by the system state.

Figure 3-2 presents one version of a hazard model in which there are two types of safety risk controls. Preventative risk controls are designed in barriers to prevent the manifestation or 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 or existing 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. A simpler explanation is that there are three ways to mitigate risk: reduce the chance of the hazard occurring; reduce the chance of the hazard causing or contributing to an incident or accident if the hazard does occur; and changing the severity of the potential outcome if the accident or incident does occur.

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.

Appendix C, *SRM Tools*, 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.

Once all hazards are identified and documented, the Analyze Safety Risk phase can begin.

3.6. Step 3: Analyze Safety Risk

3.6.1. Overview

In this step, the SRM Team determines the severity and likelihood of each effect by:

- Evaluating each hazard identified in Step 2, Identify Hazards, 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) and
- 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 safety risk.

An accident rarely results from a single failure or event. Consequently, safety risk analysis is often not a single binary (e.g., on/off, open/close, break/operate) analytical look. While they may result in the simple approach, safety 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 effect of a hazard. The SRM Team can use quantitative or qualitative methods to analyze the safety risk. Different failure modes of the system(s) can impact both severity and likelihood in unique ways.

3.6.2. 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 3-1 provides some examples of existing controls.

Table 3-1: Existing Control Examples

Controller	Pilot	Equipment/Technical Operations	Design

• 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 X (ASDE-X)
• Procedures
  − Specific SOP Reference
  − FAA Order Reference
• Triple Redundant Radio
• Controller Intervention
• Training
  − Implementation
  − Routine Periodic
• Management Oversight
	• Alert Procedures
	• 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
		• Traffic Alert and Collision Avoidance System (TCAS)
		• Ground Proximity Warning System (GPWS)
			• FAA Advisory Circulars
			• FAA Order Reference
			• Engineering Briefs

3.6.3. Determining Severity

Severity is the consequence or impact of a hazard's effect 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 safety risk associated with each hazard. It is important that the SRM Team consider all potential

outcomes in order to identify the highest risk and develop effective mitigations for each unique outcome.[16]

Table 3-2 contains the severity definitions as provided in FAA Order 8040.4. LOBs/Staff Offices may use their own definitions in their application of SRM or, if the assessment is cross-LOB, stakeholders may agree to use a different set of definitions. The categories are mutually exclusive and collectively exhaustive.

Some effects associated with a hazard may have rarely occurred or not occurred at all. However, if a hazard has resulted in an event indicating an aircraft avoided an accident but experienced imminent danger, those events may be used as the basis for a prediction of effects at all levels of severity.

Table 3-2: Severity Definitions*

Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Negligible safety effect	An unexpected unintentional effect that includes any of the following: • 1-2 minor injuries • Minor damage to manned aircraft • Substantial damage** to unmanned aircraft weighing at least 55 pounds	An unexpected unintentional effect that includes any of the following: • 1-2 serious injuries** • 3 or more minor injuries • Substantial damage** to manned aircraft • Hull loss to unmanned aircraft weighing at least 55 pounds	An unexpected unintentional effect that includes any of the following: • 1-2 fatalities without manned aircraft hull loss • Manned aircraft hull loss without fatalities • 3 or more serious injuries**	An unexpected unintentional effect that includes any of the following: • 3 or more fatalities • Manned aircraft hull loss with at least 1 fatality

* Excludes commercial space flight vehicles, crew, and participants.
** SRM Teams may refer to 49 CFR § 830.2 for definitions of serious injury and substantial damage.

3.6.4. Determining Likelihood

Likelihood is the chance of a hazard and an effect at a specific level of severity.

The SRM Team needs to consider severity in conjunction with the determination of likelihood in order to predict risk accurately. FAA Order 8040.4 provides both likelihood definitions and expected value definitions. Whether using the likelihood definitions, expected value definitions, or another LOB/Staff Office's definitions, the SRM Team should thoroughly and clearly articulate its rationale for the determined likelihood, so that decision makers understand the Team's assessment. As described in several of the tool descriptions in Appendix C, *SRM Tools*, likelihood may be thought of as the joint probability of several factors, barrier failures/successes, and events leading to an outcome of a particular severity.

Table 3-3 contains the likelihood definitions, as provided in the current version of FAA Order 8040.4. The likelihood definitions are expressed on a per-flight-hour basis, as both a probability and frequency.

[16] In accordance with FAA Order 8040.4, if the probability of an effect is less than 1×10^{-11}, it does not need to be considered.

Table 3-3: Likelihood Definitions

Category	Less than	Greater than or Equal to
Frequent – A	1	1×10^{-5} (1 per 100,000)
Infrequent – B	1×10^{-5} (1 per 100,000)	1×10^{-6} (1 per 1,000,000)
Extremely Infrequent – C	1×10^{-6} (1 per 1,000,000)	1×10^{-7} (1 per 10,000,000)
Remote – D	1×10^{-7} (1 per 10,000,000)	1×10^{-8} (1 per 100,000,000)
Extremely Remote – E	1×10^{-8} (1 per 100,000,000)	1×10^{-9} (1 per 1,000,000,000)
Improbable – F	1×10^{-9} (1 per 1,000,000,000)	1×10^{-10} (1 per 10,000,000,000)
Extremely Improbable – G	1×10^{-10} (1 per 10,000,000,000)	0

The likelihood of an effect occurring can be found by dividing the estimated number of times the effect is expected to occur by the number of flight hours in which the hazard could occur (i.e., the exposure in flight hours). The equation is displayed below.

$$Likelihood = \frac{Estimated\ or\ actual\ number\ of\ effect\ occurrances}{Exposure\ in\ flight\ hours}$$

To find the denominator of the likelihood equation, SRM Teams must determine the number of flight hours that are exposed to the hazard. The SRM Team can utilize the system state of the hazard to determine the exposure. For example, if the system state is IFR only, then only flight hours in which operations occur under IFR should be used for the exposure. When determining exposure, the SRM Team should consider factors such as the number of flight hours, the specific phases of flight, and the geographical locations where exposure is likely. Note that exposure in *flight hours* must be used in order to utilize the likelihood definitions and the risk matrices. If the safety issue is better analyzed through another unit of exposure (e.g., flights or operations), that unit must be equated to flight hours to determine the likelihood category. See Section 3.6.4.1, *Equating Different Units of Exposure to Flight Hours*, below for more information.

To determine the numerator of the likelihood equation, SRM Teams must establish, via analytical, empirical, or judgmental data, the estimated or actual number of times the effect will occur due to the hazard over the same period of time that was used for the exposure.

These results can then be used to determine the likelihood category for the hazard's effect. This equation can be used again for each effect of every hazard identified.

The likelihood equation described above is an average rate of occurrence estimate. Other estimation methods are discussed in Appendices C, *SRM Tools*, and D, *SRM Technical Definitions*, and are available for use depending on the safety issue.

3.6.4.1. Equating Different Units of Exposure to Flight Hours

As stated above, flight hours must be used as the unit of exposure in order to use the likelihood definitions and the risk matrices in FAA Order 8040.4. However, there may be safety issues for which flight hours are not the most appropriate exposure unit. For example, assessing a safety issue with risk exposure only during takeoff is better expressed through operations. In these cases, the SRM Team should utilize the most appropriate unit of exposure for the safety issue,

and then convert that unit of exposure to flight hours to establish the likelihood category and plot the hazard's effect on the risk matrix. When selecting the appropriate unit for exposure, it is essential to consider the specific characteristics of the hazard and the operational context. The chosen unit should provide a meaningful and accurate representation of the frequency and duration of exposure.

The equations and steps below will help the SRM Team determine the exposure in flight hours (i.e., the denominator in the likelihood equation in Section 3.6.4, *Determining Likelihood*) from exposure in flights, operations, or non-flight operations.

Essentially, the SRM Team will need to multiply the exposure in the unit chosen by the average number of flight hours within one of the exposure units chosen. The sections below provide equations to find the exposure in flight hours from flights, operations, and non-flight operations.

3.6.4.1.1. EQUATING FLIGHTS TO FLIGHT HOURS

If the safety issue is best assessed with flights as the unit of exposure, the following steps and equations should be used to determine the exposure in flight hours.

Step 1: Determine the number of flights exposed to the hazard.

In doing so, consider the operation type, the system state of the hazard, and the time period of the analysis in which the effect occurrences will be counted or estimated.

Step 2: Determine the average number of flight hours per flight by recording the total flight hours in any known period of time and the total number of flights in the same time period. The Team should then divide the total number of flight hours by the total number of flights, as in the equation below.

$$Average\ flight\ hours\ per\ flight = \frac{Total\ flight\ hours}{Total\ number\ of\ flights}$$

Step 3: Combine the results of Steps 1 and 2 to solve the following equation.

$$Exposure\ in\ flight\ hours = Flights\ exposed\ to\ hazard\ \times Average\ flight\ hours\ per\ flight$$

The result is the exposure in flight hours, which is the denominator of the likelihood equation.

Below is an example of equating flights to flight hours.

> An SRM Team determines that the number of flights exposed to the hazard is 8 million (8M) flights. This would complete Step 1.
>
> Between 2008 and 2018, data show that 14 CFR part 121 operators flew approximately 18M flight hours per year while flying approximately 9M flights per year. To complete Step 2, the SRM Team would perform the following equation.
>
> $$Average\ flight\ hours\ per\ flight = \frac{18M\ flight\ hours}{9M\ flights} = 2\ flight\ hours\ per\ flight$$
>
> To complete Step 3, the SRM Team would take the number of flights exposed to the hazard (8M) from Step 1 and the average flight hours per flight (2 flight hours per flight) from Step 2, and use them to solve the exposure equation, displayed below.

$$Exposure\ in\ flight\ hours = \ 8M\ flights\ \times 2\ flight\ hours\ per\ flight\ = 16M\ flight\ hours$$

Therefore, for this example, the exposure is 16M flight hours.

3.6.4.1.2. EQUATING OPERATIONS TO FLIGHT HOURS

If the safety issue is best assessed with operations as the unit of exposure, the following steps and equations should be used to determine the exposure in flight hours.

Step 1: Determine the number of operations exposed to the hazard.

In doing so, consider the operation type, the system state of the hazard, and the time period of the analysis in which the effect occurrences will be counted or estimated.

Step 2: Determine the average flight hours per operation by recording the total flight hours in any known period of time and the total number of operations in the same time period. The Team should then divide the total number of flight hours by the total number of operations, as in the equation below.

$$Average\ flight\ hours\ per\ operation = \frac{Total\ flight\ hours}{Total\ number\ of\ operations}$$

Step 3: Combine the results of Steps 1 and 2 to solve the following equation.

$$Exposure\ in\ flight\ hours = Operations\ exposed\ to\ hazard\ \times Average\ flight\ hours\ per\ operation$$

The result is the exposure in flight hours, which is the denominator of the likelihood equation.

Below is an example of equating operations to flight hours.

In Step 1, the SRM Team determines the number of takeoffs (operations) exposed to the hazard is 10M.

Between 2015 and 2020, airport runway data show that there were 15M takeoffs at the relevant airport per year, flying approximately 30M flight hours per year. To complete Step 2, the SRM Team would perform the following equation.

$$Average\ flight\ hours\ per\ operation = \frac{30M\ flight\ hours}{15M\ operations} = 2\ flight\ hours\ per\ operation$$

To complete Step 3, the SRM Team multiplies the takeoffs (operations) exposed to the hazard by the average flight hours per operation.

$$Exposure\ in\ flight\ hours = 10M\ operations \times 2\ flight\ hours\ per\ operation = 20M\ flight\ hours$$

Therefore, for this example, the exposure is 20M flight hours.

3.6.4.1.3. EQUATING NON-FLIGHT OPERATIONS TO FLIGHT HOURS

If the safety issue is best assessed with non-flight operations as the unit of exposure, the following steps and equations should be used to determine the exposure in flight hours.

Step 1: Determine the number of non-flight operations exposed to the hazard.

In doing so, consider the operation type, the system state of the hazard, and the time period of the analysis in which the effect occurrences will be counted or estimated.

Step 2: Determine the average flight hours per non-flight operation by recording the total flight hours in any known period of time and the total number of non-flight operations in the same time period. The Team should then divide the total number of flight hours by the total number of non-flight operations, as in the equation below.

$$Average\ flight\ hours\ per\ non\text{-}flight\ operation = \frac{Total\ flight\ hours}{Total\ number\ of\ non\text{-}flight\ operations}$$

Step 3: Combine the results of Steps 1 and 2 to solve the following equation.

$$Exposure\ in\ flight\ hours = Non\text{-}flight\ operations\ exposed\ to\ hazard \times Average\ flight\ hours\ per\ non\text{-}flight\ operation$$

The result is the exposure in flight hours, which is the denominator of the likelihood equation.

Below is an example of equating non-flight operations to flight hours.

> In Step 1, the SRM Team determines the number of non-flight refueling operations exposed to the hazard is 5M.
>
> Between 2020 and 2023, airport data show that there were 3M refueling operations at the relevant airport per year, supporting approximately 15M flight hours per year, as determined from fuel sales and average consumption rate. To complete Step 2, the SRM Team would perform the following equation.
>
> $$Average\ flight\ hours\ per\ non\text{-}flight\ operation = \frac{15M\ flight\ hours}{3M\ refueling\ operations} = 5\ flight\ hours\ per\ refueling\ operation$$
>
> To complete Step 3, the SRM Team multiplies the refueling operations exposed to the hazard by the average flight hours per refueling operation.
>
> $$Exposure\ in\ flight\ hours = 5M\ refueling\ operations\ \times 5\ flight\ hours\ per\ operation = 25M\ flight\ hours$$
>
> Therefore, for this example, the exposure is 25M flight hours.

3.6.4.2. Expected Value Definitions and Use

When the SRM Team wants to use expected value (see Appendix D, *Technical Definitions*, for more information on expected value) to determine likelihood, FAA Order 8040.4 also provides a calendar-based expected value table (see Table 3-4 below). The following caveats apply when using the provided Expected Value Definitions in the order:

- The assumed exposure is 10 million flight hours per year, and
- If the data analysis is largely reliant on judgmental data, the analysis cannot reach a category less than Improbable, as judgmental data cannot reliably be estimated to that level.

Table 3-4: Expected Value Definitions

Category	Time/Calendar-based Occurrences Based on an average of 10 million flight hours per year
Frequent – A	Expected to occur more than once every 4 days
Infrequent – B	Expected to occur one time every 4 days to more than one time every 1 month
Extremely Infrequent – C	Expected to occur one time every 1 month to more than one time every 1 year
Remote – D	Expected to occur one time every 1 year to more than one time every 10 years
Extremely Remote – E	Expected to occur one time every 10 years to more than one time every 100 years
	Or unlikely, but possible to occur in the life of an aircraft
Improbable – F	Expected to occur one time every 100 to 1,000 years
	Or so unlikely, it can be assumed occurrence may not be experienced in the life of an aircraft type
Extremely Improbable – G	Expected to occur less than once every 1,000 years*

* If the analysis is largely reliant on judgmental rather than empirical or analytical data, then the analysis must not reach a likelihood less than Improbable.

While the above definitions can only be used when the exposure is estimated at an average of 10 million flight hours per year, an SRM Team can easily determine expected values from the Likelihood Definitions (Table 3-3 above), as long as the Team has the estimated exposure. The Team can use the Expected Value Tool on the FAA SRM Intranet to find the expected value equivalent. The tool is also discussed in Appendix C, *SRM Tools*.

3.6.4.3. Utilizing Calendar-based Metrics

There may be times when it is helpful to estimate likelihood in a calendar-based unit or to communicate the likelihood to decision makers using a calendar-based metric. In these cases, FAA Order 8040.4 has provided information on how to convert a calendar-based metric to a probability, as well as a probability to a calendar-based metric.

When converting a calendar-based metric to a probability, the SRM Team must determine the number of flight hours exposed to the hazard within that time period. That number, along with the number of effect occurrences in the time period, are entered into the following equation to determine the probability.

$$Probability = \frac{Number\ of\ effect\ occurrences\ in\ time\ period}{Number\ of\ exposed\ flight\ hours\ in\ time\ period}$$

When converting a probability to a calendar-based metric, the SRM Team must first decide the time period in which they wish to know the number of effect occurrences, and then determine the number of exposed flight hours in the chosen time period. The exposure and probability entered into the following equation will provide the SRM Team with the number of effect occurrences within the time period chosen.

$$Calendar\text{-}based\ metric = Number\ of\ affected\ flight\ hours\ in\ time\ period \times Probability\ of\ effect\ occurring$$

Below is an example of how to determine a calendar-based metric from a probability and exposure.

> An SRM Team determines that the number of flight hours exposed to the hazard is 15M flight hours per year. The SRM Team also determined via data that the probability of an effect occurring is 0.00001 (or 1×10^{-5}). The SRM Team wants to provide a calendar-based metric for executives; the Team would use the equation below to find the expected value.

$$Calendar\text{-}based\ metric = 15M\ flight\ hours\ per\ year \times 0.00001 = 150\ effects\ occurring\ per\ year$$

3.7. Step 4: Assess Safety Risk

3.7.1. Overview

In the Assess Safety Risk step, the SRM Team:

- Plots each hazard's associated safety risk per effect (as identified in Step 3, Analyze Safety Risk) on the risk matrix, using severity and likelihood;
- Determines which effects associated with the hazard represent high, medium, and low risk; and
- Determines the need for risk control development based on level of safety risk.

3.7.2. 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 FAA Order 8040.4 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. These processes may include evaluating design constraints such as single points of failure or common cause failures, and risk levels may be adjusted to account for these conditions when appropriate. Organizational processes may also assess risk without using a risk matrix (for example, evaluation against the probability of a fatal effect). 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. It can help decision makers understand where new/current risk falls relative to other safety risk in the system and can be a useful aid to discuss and prioritize mitigation action.

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.

3.7.3. Types of Risk

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

3.7.4. Choosing a Risk Matrix

FAA Order 8040.4 contains two different risk matrices—one for commercial aviation and one for general aviation (GA). SRM Teams should choose the matrix that most accurately reflects the type of operation and potential safety effects of the hazard assessed. As an example, if a hazard occurs during a GA operation but the effect could impact commercial operations, the SRM Team should use both matrices and assess GA and commercial operations separately.

FAA Order 8040.4 explains the intention of each risk matrix in Appendix C, Paragraph 6b:

> The commercial aviation guidelines are intended to be minimum standards when assessing large air transport operations and aircraft systems providing air transportation for 10 or more seats, such as those operated by 14 CFR parts 121, 125, and 129 commercial air carriers. GA guidelines are intended to establish the minimum standard for all other aviation segments or combinations of segments. This includes, but is not limited to, all 14 CFR part 91 operations, small aircraft operated by part 121 certificate holders, part 135 commuters, and small for-hire operations such as those conducted under parts 107, 133, and 137.

Figures 3-3 and 3-4 show the risk matrices in FAA Order 8040.4.

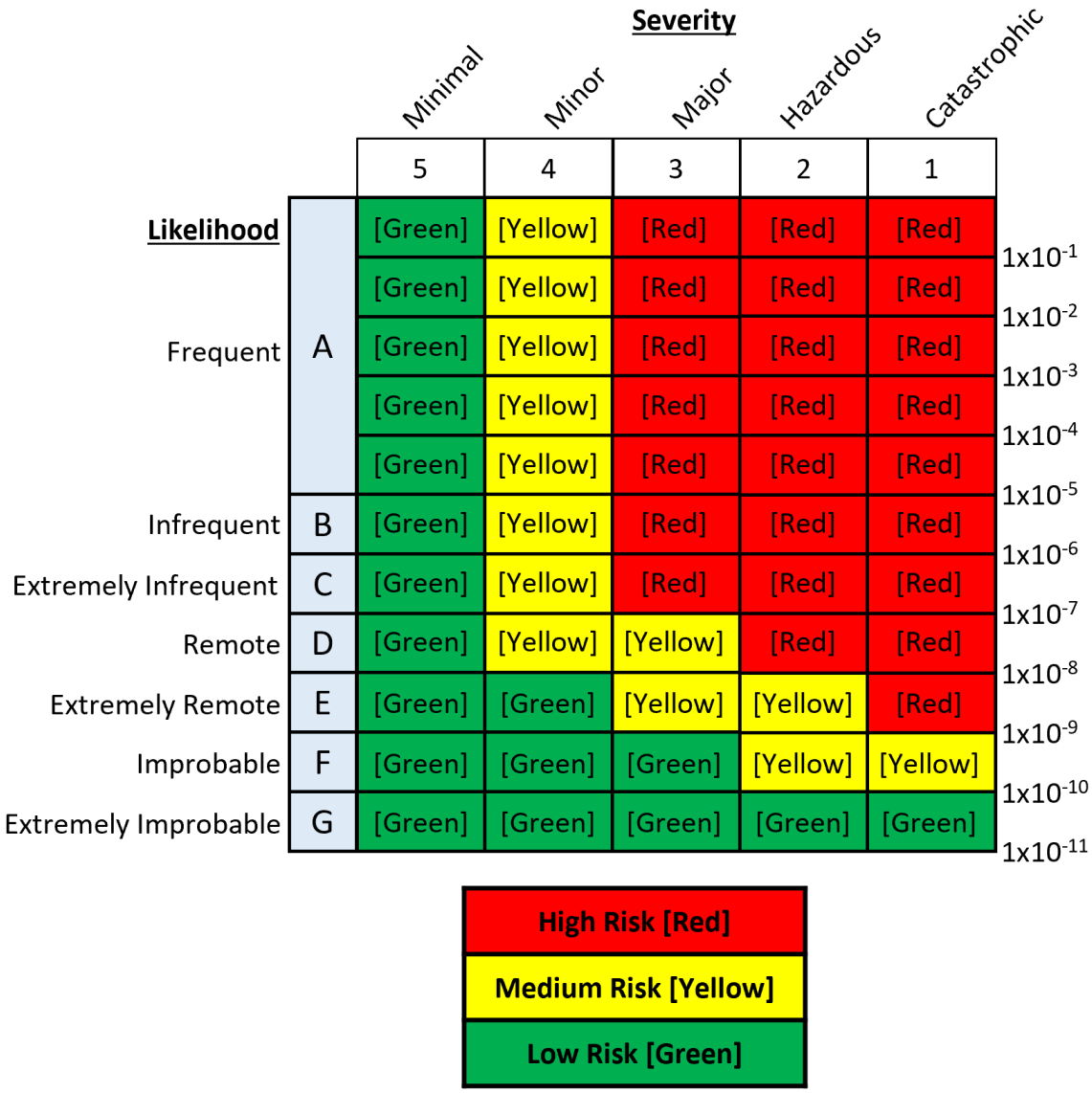


Figure 3-3: Risk Matrix for Commercial Aviation

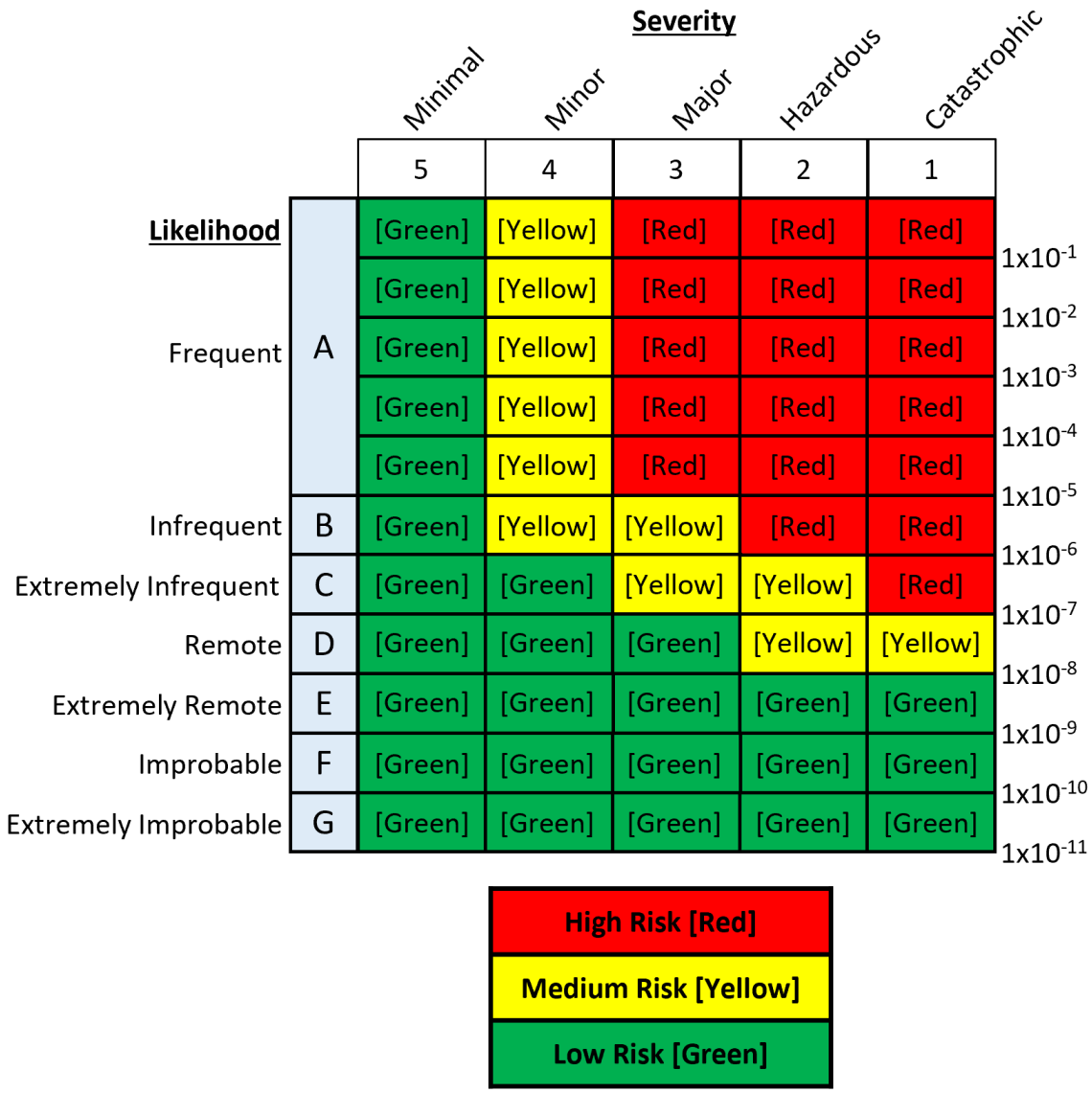


Figure 3-4: Risk Matrix for General Aviation

3.7.5. 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** means severity and likelihood map to the red cells in the risk matrix (see Figures 3-3 and 3-4). 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** means severity and likelihood map to the yellow cells in the risk matrix (see Figures 3-3 and 3-4). Although this safety risk is acceptable without additional mitigation, tracking and monitoring are required. However, it is desirable to achieve the lowest practicable risk levels (factoring in the principles of appropriate resource management).

- **Low Risk** means severity and likelihood map to the green cells in the risk matrix (see Figures 3-3 and 3-4). 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 effects according to their associated safety risk levels (illustrated by where they fall on the risk matrix).
- To plot a hazard's effect on the risk matrix, select the appropriate severity column (based on the severity definitions) and then plot the hazard's effect where the likelihood falls on the logarithmic scale.
- If any of the plotted points fall within the red region, the safety risk associated with the hazard is high; if any of the plotted points fall within the yellow region with none in the red, the safety risk associated with the hazard is medium; otherwise, the risk is low.

If any plotted point falls close to the dividing line between Low to Medium or Medium to High risk, the SRM Team should consider calculating the cumulative probability of effects at each level of severity. This is done by plotting the sum of the probability of the effect and the probabilities of all other effects that are more severe. This will result in the probability of all effects that are at least as severe as the category in question.

3.8. Step 5: Control Safety Risk

3.8.1. Overview

In this step, the SRM Team develops and manages options to deal with safety risk (from Step 4, Assess Safety Risk). These options are safety risk controls. A safety risk control (also referred to as a mitigation or control or safety recommendation/requirement) 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. Effectively mitigating safety 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 safety recommendations for managing the safety risk associated with a hazard. These recommendations become actions that reduce the risk of the hazard's effects on the system (e.g., human interface, operation, equipment, procedures) or eliminate the hazard. Regardless of who develops safety recommendations 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. 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. Note that safety recommendations assigned to external organizations are not tracked by the FAA. SRM Teams

should prioritize FAA actions and/or design a recommendation for the FAA to oversee the external action, if possible.

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 Monitoring Plan and are often the subject of research and development activities. The SRM Team can use Safety Order of Precedence principles (see Section 3.8.6) to focus on mitigations that produce the greatest safety improvement for the level of effort/investment (e.g., prioritize mitigations that offer "the most bang for the buck").

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)

When developing safety recommendations, SRM Teams, OPRs, and Facilitation Teams should employ the following best practices:

- Determine and designate Mitigation Owner POCs[17] during the SRM phase to ensure efficient and effective communication with the HIRMT Program Manager.
- Ideally each mitigation would have one Mitigation Owner; however, at times co-owners are assigned. Multiple Mitigation Owners should work jointly, and when possible, should identify a lead organization that would be responsible for coordinating with the other co-owner organization(s). If the co-owners need to work separately, the SRM Team should consider splitting the mitigation into multiple mitigations with one owner each.
- Facilitators should encourage the SRM Team to categorize the recommendations according to estimated timeframe (e.g., short [6 months], mid [2 years], and long [beyond 2 years] term) to ensure decision maker awareness that initial/interim risk could remain until the mitigations with longer timeframes are implemented. If possible, the SRM Team should also consider highlighting the most critical mitigations or category of mitigations and their impact on the overall safety issue risk.
- Consider adding specific exit criteria for mitigation completion. For example, if the mitigation is training, specify whether it is complete when the training is planned, developed, or delivered.
- Encourage the SRM Team to identify and recommend interim actions to control risk while awaiting implementation of more permanent mitigations (e.g., immediate actions FAA executive stakeholders could put in place to address the risk). These interim actions should be included with the Safety Recommendations.
- The FAA does not track recommendations that are owned by external organizations (both governmental and non-governmental entities). SRM Teams should prioritize FAA actions and/or design a recommendation for the FAA to oversee the external action, if possible.

[17] See Appendix A, *Roles and Responsibilities*, for more information on the Mitigation Owner role.

3.8.2. Evaluate Proposed Controls and Determine Predicted Residual Risk

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. The SRM Team assesses the hazards and corresponding effects, utilizing the likelihood and severity definitions in FAA Order 8040.4, as if all safety recommendations have been implemented. The resulting risk level is the predicted residual risk. The predicted residual risk is then plotted on the risk matrix. 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 the safety risk associated with the hazard will be mitigated to an acceptable level.

Note that the predicted residual risk may be updated if some of the safety recommendations identified by the SRM Team are rejected or modified by FAA management. See Section 4.5., *Reassess Predicted Residual Risk and Develop Safety Risk Assessment Report Addendum*, for more information.

3.8.3. Develop a Monitoring Plan

As part of the SRM documentation, the SRM Team develops a Monitoring Plan, which the OPR is responsible for completing and therefore must be approved by the OPR. This plan is established to:

- Confirm the risk controls have the desired effect;
- Enable monitoring of the effectiveness of those controls; and
- Confirm safety performance targets are met.

It may also be used to conduct post-implementation assessments to verify the results of the analysis. Table 3-5 shows a sample Monitoring Plan. The Monitoring Plan template can be found in the HAW Template (see Appendix B, *Templates*, for more information).

Table 3-5: Sample Monitoring Plan

Monitoring Activities	Reporting Frequency	Reporting Duration	Safety Performance Targets
Description of how the risk associated with each of the hazards identified will be monitored	*How often the monitoring activities listed in the previous column will be tracked*	*Length of time that the monitoring activities will be tracked*	*Measurable goals that will be used to verify the implementation of the safety recommendations and validate the predicted residual risk*
Example 1: Review X data source for Emergency Autoland activation events	Example 1: Monthly, quarterly, etc.	Example 1: Three years	Example 1: Zero Emergency Autoland activation events with catastrophic outcomes
Example 2: Track and monitor availability of equipment Z to users	Example 2: Monthly, quarterly, etc.	Example 2: Five years	Example 2: Safety performance measure is 98% or higher availability

The SRM Team should designate a Monitoring Plan Data Owner,[18] who will collect the specific data items identified during the execution of the Monitoring Plan and provide it to the OPR. The

[18] See Appendix A, *Roles and Responsibilities*, for more information on the Monitoring Plan Data Owner role.

SRM Team should also, if possible, specify the data source/database that will be used by the Monitoring Plan Data Owner to collect the data. The Monitoring Plan Data Owner will review the Monitoring Plan and provide feedback to the OPR and SRM Team on whether the identified data can feasibly be collected from the specified data source/database. This review can either be performed during the SRM Team meetings, if the Monitoring Plan Data Owner is in attendance, or during the SRM Team review of the Safety Risk Assessment Report.

While the reporting duration listed in the Monitoring Plan begins after all approved mitigations have been implemented, monitoring activities should begin as soon as the Safety Risk Assessment Report, or Addendum, if applicable, is signed and entered into HIRMT. This ensures that the FAA has full visibility of any activity surrounding the safety issue throughout the entire SRM process.

When developing the Monitoring Plan, SRM Teams, OPRs, Facilitators, and Documentation Analysts should employ the following best practices:[19]

- SRM Teams may opt to include an OPR signature block to the Monitoring Plan to improve accountability for executing Monitoring Plan activities, in addition to the OPR signature for the final Safety Risk Assessment Report or Addendum.
- Provide sufficient, relevant detail in the Monitoring Plan to ensure that expectations for data collection and analysis can be realistically met. Details should specify the exact data that should be collected, the Monitoring Plan Data Owner(s), and the method in which data will be collected and monitored. Note that the Monitoring Plan Data Owner (organization responsible for collecting data identified in the Monitoring Plan) may be different from the organization responsible for analyzing the data and determining safety performance. Accessible/relevant data sources and reliable methods to collect and analyze data help to ensure the Monitoring Plans are actionable.
- Monitoring of the safety issues should begin once the Safety Risk Assessment Report Addendum has been signed. The reporting durations defined in the Monitoring Plan should be continued for the timeframe specified once all mitigations have been implemented.
- The organization responsible for data collection and monitoring is not always present at the SRM Team meeting to provide input on exactly what data can be collected. If those responsible for data collection are not present at the meeting, an alternative method to allow the responsible organization to provide feedback on the initial Monitoring Plan proposed by the SRM Team should be employed. Doing so would help ensure the collection and monitoring expectations are understood and executable.
- If the SRM Team made an assumption during the assessment that would vastly affect the outcome of the assessment if proved incorrect, the SRM Team should include a monitoring activity that assesses the validity of the assumption, if possible.
- The Safety Performance Targets in the Monitoring Plan should be set within the range of the predicted residual risk identified by the SRM Team.

Note that the Monitoring Plan may be updated if some of the safety recommendations identified by the SRM Team are rejected or modified by FAA management. See Section 4.5., *Reassess Predicted Residual Risk and Develop Safety Risk Assessment Report Addendum*, for more information.

[19] In accordance with FAA Order 8040.4, low risk hazards are not required to have a Monitoring Plan.

3.8.3.1. Safety Performance Targets

Safety performance targets 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 target when it develops the Monitoring Plan. The sources of data used for the SRM Team's assessment 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.

When developing safety performance targets, the SRM Team should review the entire event sequence and not necessarily focus on the highest risk outcome. Precursors to an incident or accident may provide additional insight to safety performance as incidents or accidents may be infrequent. An SRM Team must define the safety performance targets in order to confirm the safety risk controls have the desired effect.

3.8.4. Strategies for Managing Risk

Risk mitigation requires management's informed decision to approve, fund, schedule, and implement one or more risk mitigation strategies. Risk acceptance is a management decision. 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 (see Section 3.8.3, *Develop 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.

3.8.4.1. Risk Transfer Strategy

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) and entered into HIRMT.

Examples of risk transfer may include:

- Transfer of aircraft separation responsibility in applying visual separation from the Terminal Radar Approach Control Facility (TRACON) to the Air Traffic Control Tower (ATCT) via Letter of Agreement
- 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 further 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 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 entity.

3.8.4.2. 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.

3.8.4.3. Risk Control Strategy

A safety risk control is a means to reduce or eliminate the effects of hazards. Controls may include process design, equipment modification, work procedures, training, or protective device. A control that has been approved for implementation by FAA management is a safety requirement. Controls can be complex or simple, but all controls must be written with sufficient detail to allow their impact on the safety risk to be assessed.

A risk control strategy helps to develop options and alternatives for decision makers to take actions that lower or eliminate the risk. Examples include implementing additional policies or procedures, developing redundant systems and/or components, using alternate sources of production, and changes to regulatory text.

3.8.5. Defenses in Depth

3.8.5.1. Designing an Error Tolerant System

Given the complex interplay of human, material, and environmental factors in operations, the complete elimination of safety risk is an unachievable goal. Even in organizations with the best training programs and a positive safety culture, human operators will occasionally make errors and 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 contains 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 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 3-5 illustrates how an accident event must penetrate all defensive layers.

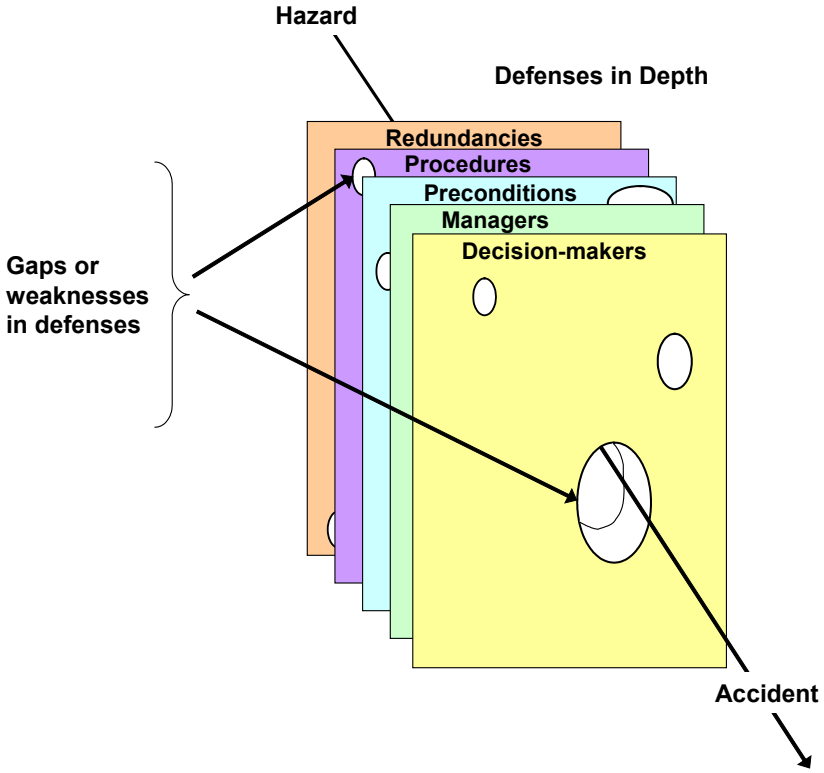


Figure 3-5: Defenses in Depth Philosophy

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.

3.8.5.2. Detecting and 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 the event 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

3.8.5.3. Effect of Hardware and Software on Safety

System designers generally design the hardware and software components of a system to meet specified levels of reliability, maintainability, and availability (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 multiple paths, making the service unavailable. An example of physical diversity is the requirement to bring commercial power into Air Route Traffic Control Centers (ARTCCs) through two different locations. In the event of a fire or other issue in one location, the alternate path would still provide power, which increases the likelihood that service would remain available.

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

3.8.5.4. Human Element's Effect on Safety

Sub-system designers must design the human-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-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.

3.8.6. 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 safety risk. The methods for reducing safety risk generally make up the Safety Order of Precedence in the following order of preference:

1. Design for minimum risk,
2. Incorporate safety devices,
3. Provide warning, and
4. Develop procedures and training.

Whenever possible, the highest priority is to design for minimum risk at the earliest stages of system development (e.g., early safety risk assessments for an acquisition). Appendix C, *SRM Tools*, provides more information on the Safety Order of Precedence.

Chapter 4. Documenting Cross-LOB Safety Risk Assessments and Obtaining Mitigation Approval

This chapter describes the steps to document cross-LOB assessments, as well as the steps for management to approve mitigations. Figure 4-1 below depicts the process for documenting cross-LOB safety risk assessments and obtaining mitigation approvals.

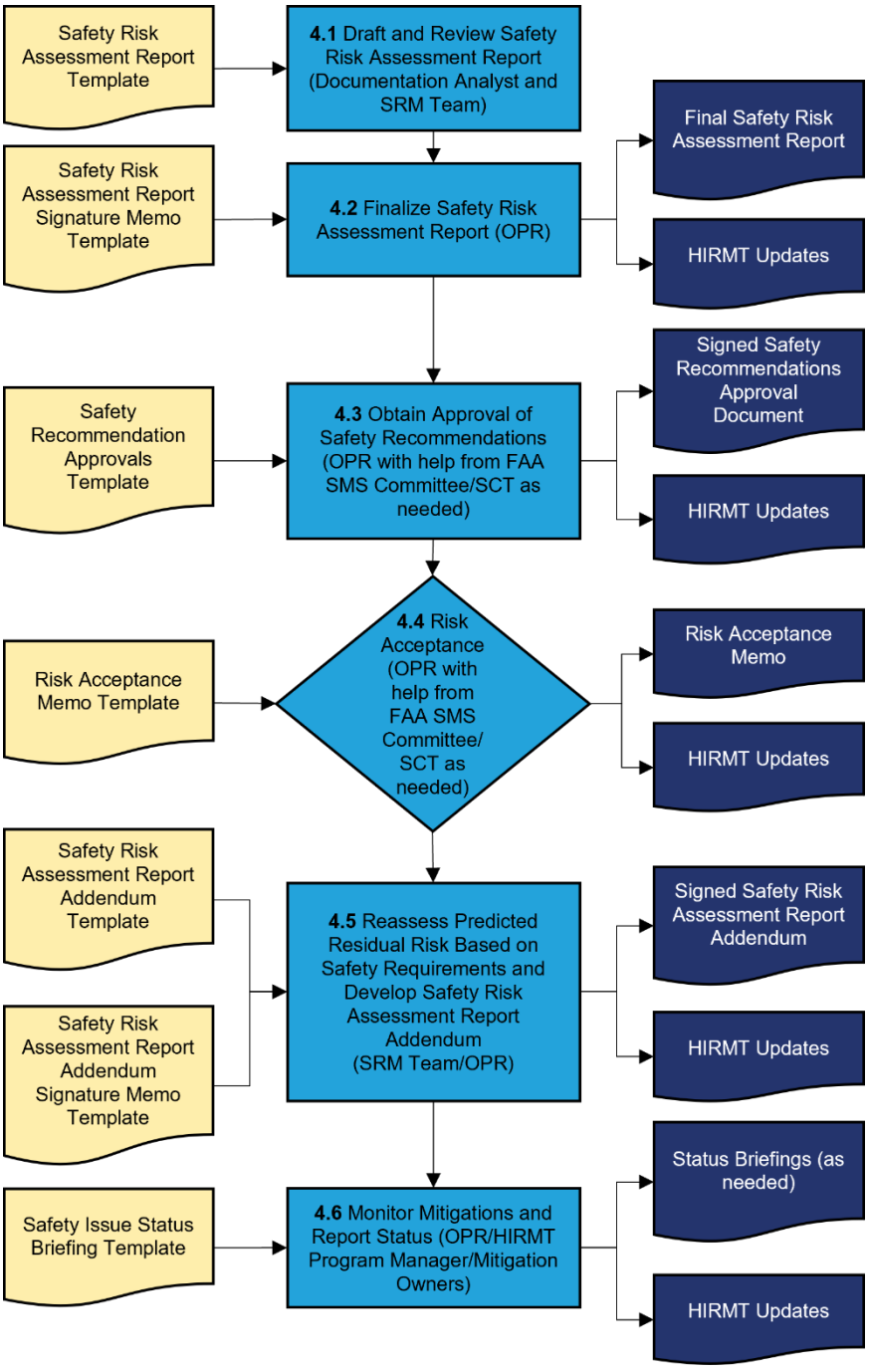


Figure 4-1: Documenting Cross-LOB Safety Risk Assessments and Obtaining Mitigation Approvals Flow Chart

4.1. Draft and Review Safety Risk Assessment Report

The draft HAW and/or other SRM draft documents will be provided to the SRM Team for review shortly after the conclusion of the SRM Team meeting to verify that the assessment was correctly recorded. The Documentation Analyst will then begin drafting the Safety Risk Assessment Report. If the SRM Team identifies a serious issue that is outside the scope of the risk assessment, then the Team can document the issue in an appendix to the Safety Risk Assessment Report and share it with the appropriate stakeholders and the FAA SMS Committee.

Once the draft Safety Risk Assessment Report is complete, the SRM Team reviews it and reaches concurrence (or as close as possible) on the results. SRM Team members provide comments on the draft Safety Risk Assessment Report to the OPR POC using the Comment Matrix Template (see Appendix B, *Templates*). The OPR POC leads a sub-team to resolve Team comments. Comments and resolutions are provided back to the commenters. The SRM Team should strive to reach consensus, but there may be instances in which not all SRM Team members agree on the results of the safety risk assessment. In those cases, the Team documents the results of the assessment, records the comments and other opinions, and delivers the results to the decision maker. Records of comments and other opinions are appended to the Safety Risk Assessment Report, if necessary, using the Record of Comments and Other Opinions Template (see Appendix B, *Templates*).

Once the SRM Team has reviewed the Safety Risk Assessment Report and the OPR POC deems it complete, a peer/technical review is conducted to assure the report is complete and accurate and that the appropriate process was followed during the development of the report. Individuals, other than those who have conducted SRM, should perform the peer review. These individuals should have similar expertise as the SRM Team members. An SCT member can conduct the peer review or the SCT can designate an FAA senior technical expert(s) to review the draft Safety Risk Assessment Report for completeness and accuracy and to assure that the appropriate process was followed.[20] The peer reviewer(s) will sign the cover memo of the report indicating that the appropriate process was followed, and the report appears to be complete and accurate.

If the Monitoring Plan is included in the Safety Risk Assessment Report, the Monitoring Plan Data Owner must review the Monitoring Plan before the Safety Risk Assessment Report can be finalized.

4.2. Finalize Safety Risk Assessment Report

After the peer review is conducted, the OPR POC approves the Safety Risk Assessment Report.[21] Safety Risk Assessment Report approval indicates that the report was developed properly, that hazards were systematically identified, and that safety risk was appropriately assessed. Safety Risk Assessment Report approval does not constitute acceptance of the safety risk associated with the safety issue or approval to implement the mitigations/change.

Approval signatures are not part of the Safety Risk Assessment Report. Instead, the signatures are recorded separately on the Safety Risk Assessment Report Signature Memo Template (see Appendix B, *Templates*) with the Safety Risk Assessment Report attached. To finalize the

[20] The FAA SMS Committee acknowledges that affected stakeholders may require an independent peer review within their respective organizations.
[21] The FAA SMS Committee acknowledges that affected stakeholders may require additional approvals based on their organizational requirements.

Safety Risk Assessment Report, the OPR Manager signs the memo accompanying it, indicating agreement that the findings are valid and accurate, and the process was followed. The OPR POC coordinates with the HIRMT Program Manager to have the Safety Risk Assessment Report and applicable signature pages uploaded into HIRMT for documentation purposes.

If the SRM Team was able to develop the Monitoring Plan for the Report, the OPR must also approve and provide a signature on the Monitoring Plan within the Safety Risk Assessment Report. If the SRM Team has not yet developed the Monitoring Plan, the OPR will sign and approve the Monitoring Plan in either the Safety Risk Assessment Report Addendum or the Safety Recommendation Approvals document.

Once the Safety Risk Assessment Report is finalized, the OPR should coordinate with the HIRMT Program Manager to enter the report into HIRMT. The OPR should also brief the FAA SMS Committee on the status of the safety issue using the Safety Issue Status Briefing Template (see Appendix B, *Templates*).

4.3. Obtain Approval of Safety Mitigations

The OPR determines the appropriate management official(s) to approve the mitigations. If the OPR cannot make that determination, the OPR works with the FAA SMS Committee and/or the SCT to determine the appropriate management official(s) to approve mitigations.

The OPR POC is responsible for coordinating mitigation approvals. The OPR POC may brief the appropriate management official(s) within the organization responsible for implementing the mitigations (i.e., Mitigation Owners) to request approval of the proposed safety recommendations. The Mitigation Owners sign to accept and implement the recommendations in the Safety Recommendation Approvals document. In addition to the signature, the Mitigation Owners must provide an expected implementation date for the mitigations that are approved, as well as a Mitigation Owner POC who will coordinate with the HIRMT Program Manager for status updates. Approval and signature by the Mitigation Owner indicates commitment to implement the safety risk mitigations/controls and thereby converts the safety recommendation into a safety requirement.

Once approvals and signatures are obtained, the OPR POC coordinates with the HIRMT Program Manager to have the Safety Recommendation Approvals Document and applicable signatures uploaded into HIRMT for documentation purposes.

Note: If there is disagreement on the mitigations or the responsibility for implementing them, the disagreement can be escalated according to the process outlined in Chapter 6, *Escalation of SRM-Related Concerns or Disagreements*.

Each mitigation is documented in HIRMT. In coordination with each Mitigation Owner, the HIRMT Program Manager updates the HIRMT database with the mitigation implementation status updates on a regular basis. Once all mitigations are operational, they will be monitored for their effect on the aerospace system.

4.4. Risk Acceptance

As with the preceding section, the OPR determines the appropriate management official(s) to accept safety risk (i.e., the Risk Accepter[s]). If the OPR cannot make that determination, the OPR works with the FAA SMS Committee and/or the SCT to determine the Risk Accepter(s). Table 2-1 within FAA Order 8040.4 shows safety risk acceptance responsibility based on the safety risk level of the hazard. When risk mitigation strategies cross LOBs/Staff Offices, the

stakeholder organizations must approve documentation and accept risk. When the responsibility for managing the safety risk spans across more than one LOB or Staff Office, the residual safety risk must be accepted by the appropriate management official in each affected FAA organization. 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; and
- Evaluate all such cases individually.

The OPR POC works with the SRM Team Facilitator and SRM Team members to make the Risk Accepter aware of the risk level via a briefing or memo. In order to document risk acceptance, the Risk Accepter signs the Risk Acceptance Memo (see Appendix B, *Templates*) affirming any decisions made and confirming risk acceptance. Note that the signature is for documentation/record purposes only. Risk acceptance for safety issues, as defined in FAA Order 8040.4, occurs when the Risk Accepter is informed of the risk and makes the decision to either allow the situation to continue without taking additional action or decides to implement additional risk controls. Risk acceptance for planned changes occurs when the Risk Accepter makes the decision to implement the planned change without additional mitigation. However, planned changes cannot proceed without a risk acceptance signature. Remember that when an individual or organization “accepts” a risk, it does not mean that the safety risk is eliminated. Some level of safety 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.

Once risk acceptance signature(s) are obtained, the OPR POC coordinates with the HIRMT Program Manager to have the signed Risk Acceptance Memo uploaded into HIRMT for documentation purposes.

4.5. Reassess Predicted Residual Risk and Develop Safety Risk Assessment Report Addendum

Once the safety recommendations from the SRM Team have been converted into safety requirements via Mitigation Owner approval and signature, the OPR works with the SRM Facilitator to determine whether the SRM Team must meet again to reassess the predicted residual risk. If the Mitigation Owner(s) approved all the safety recommendations with no modifications and the SRM Team was able to develop the Monitoring Plan, the SRM Team does not need to meet again, and the safety issue can continue to the next step. However, if some of the safety recommendations were modified or rejected, the SRM Team should meet again to modify the predicted residual risk based on the safety requirements that were approved and will be implemented. Any modifications to the predicted residual risk or Monitoring Plan will be documented in the Safety Risk Assessment Report Addendum.

As with the Safety Risk Assessment Report, the SRM Team reviews and provides comments on the Addendum. The OPR POC leads a sub-team to resolve Team comments, and the comments and resolutions are provided back to the commenters. The Addendum is peer reviewed and approved by the OPR POC and is finalized in the same way as the Report, via memo signed by peer reviewers and the OPR Manager.

The OPR POC works with the SRM Team Facilitator(s) to update the risk acceptance memo and obtain the signature of the Risk Accepter. The Risk Accepter's signature indicates acceptance of the safety risk associated with the safety issue that is expected to remain once the safety requirements are implemented. If the Risk Accepter determines that the residual risk is not acceptable, the safety requirements are redesigned or new safety recommendations 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, 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.

The OPR POC again coordinates with the HIRMT Program Manager to enter the addendum and risk acceptance memo into HIRMT. The OPR then briefs the FAA SMS Committee on the status of the safety issue using the Safety Issue Status Briefing Template (see Appendix B, *Templates*).

4.6. Monitor Hazards and Mitigations and Report Status

As part of conducting SRM, the SRM Team creates a Monitoring Plan to confirm that the risk controls have the desired effect/are effective (see Section 3.8.3, *Develop a Monitoring Plan*). The OPR is responsible for implementing the Monitoring Plan.

The OPR is responsible for briefing its management and the FAA SMS Committee on the status of the safety issue using the Safety Issue Status Briefing Template. The frequency of updates to management will depend on the risk level and/or visibility of the safety issue. The OPR should schedule updates to coincide with the FAA SMS Committee and FAA SMS Executive Council calendar, as needed. The OPR must provide periodic updates to the HIRMT Program Manager on the status of mitigation implementation, monitoring activities, and the results of the monitoring activities. The HIRMT Program Manager will publish monthly reports that include the status of mitigations and monitoring activities; the reports will be presented to FAA SMS management on a regular basis.

If one or more of the hazards identified was medium-risk or high-risk, a Monitoring Plan must be completed before the safety issue can be closed. The FAA SMS Committee monitors the reporting and closing of the safety issue in HIRMT.[22] For cross-organizational safety issues, the OPR coordinates with the appropriate Mitigation Owners, Risk Accepters, and the FAA SMS Committee to determine when the HIRMT record can be closed (see Section 5.3, *Step 3: Safety Issue Closure*).

There may be times when an SRM Team is asked to reconvene, including but not limited to the following circumstances:

- Management requests alternative controls than those proposed in the Safety Risk Assessment Report;
- Through monitoring, the FAA observes that hazard controls are not producing the expected results;
- New safety data becomes available; or
- Management determines that it wants a broader or different scope of safety risk assessment on a safety issue (e.g., broader system analysis, additional stakeholders, change in assessment's focus).

[22] This guidance pertains to cross-LOB SRM; however, HIRMT can also be used to track and monitor organization-level safety issues and others not deemed ASL.

Chapter 5. Mitigation Performance Monitoring Process

This chapter describes a process for monitoring the performance of mitigations for FAA-level safety issues after a safety risk assessment is performed. The Mitigation Performance Monitoring Process starts at the completion of the safety risk assessment, when an individual or SRM Team finalizes the Safety Risk Assessment Report and Addendum, if applicable. The process culminates in verification of the predicted residual risk of the safety issue which leads to the issue being "Closed."

The Mitigation Performance Monitoring Process is a high-level, repeatable FAA-level process for establishing relevant and measurable safety performance targets for FAA-level safety issues, as well as a means for measuring safety performance using the HIRMT system. Figure 5-1 depicts the high-level process flow for tracking the implementation of mitigations resulting from FAA-level SRM activities, monitoring the performance relative to the safety targets identified in SRM Monitoring Plans, and addressing issues that arise while following the tracking and monitoring processes.

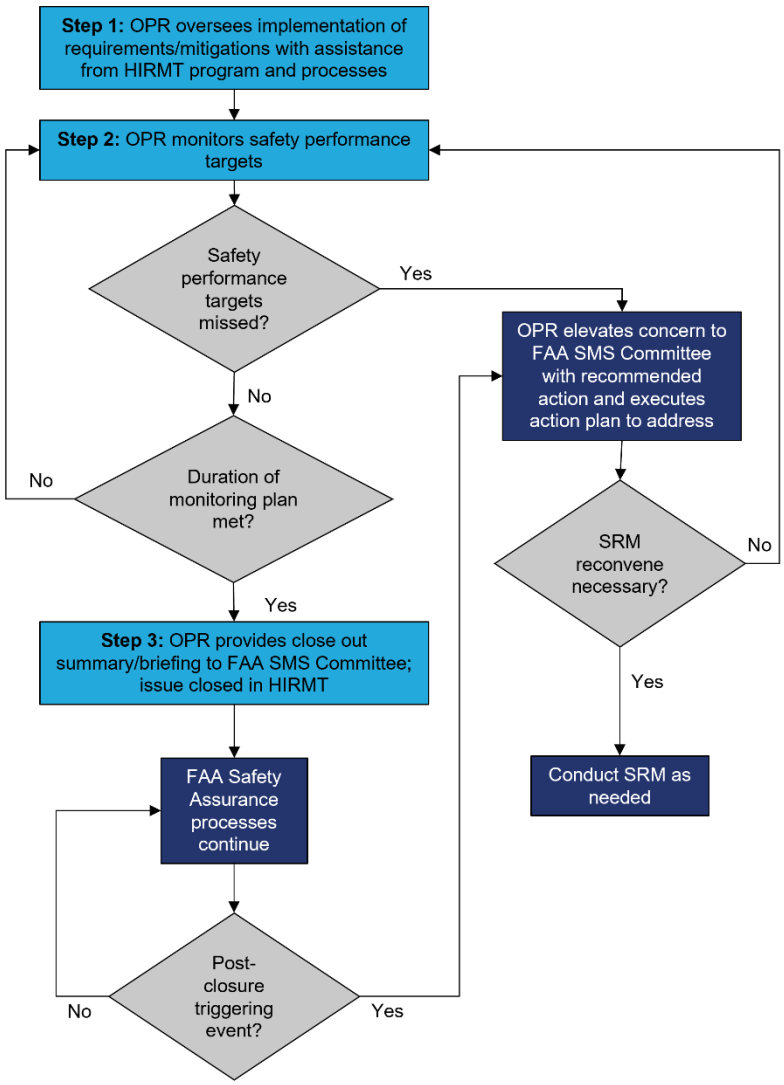


Figure 5-1: Mitigation Performance Monitoring Process Flow

5.1. Step 1: Implementation of Requirements/Mitigations

After an individual or SRM Team finalizes the Safety Risk Assessment Report and Addendum, the OPR is responsible for ensuring that mitigations are implemented, and that mitigation status is regularly communicated to the HIRMT Program Manager and the FAA SMS Committee.

The OPR, and/or appropriate Mitigation Owner(s), should brief the SCT and/or the FAA SMS Committee (or the AVSSMS Coordination Group for AVS-level safety issues) when challenges with a safety mitigation arise or if there is a delay in expected implementation dates. If the Mitigation Owner is presenting, the OPR(s) should be encouraged to accompany the Mitigation Owner(s) to ensure OPR awareness and oversight.

5.2. Step 2: Monitoring of Safety Performance Targets

The OPR is required to conduct safety assurance and is responsible for monitoring safety performance targets, as established in the issue's Monitoring Plan, throughout the duration of the Monitoring Plan, with support from the HIRMT Program Manager and HIRMT processes.

The Monitoring Plan is organized by the hazards identified in the safety risk assessment. Safety performance targets are assigned to each hazard and are monitored throughout the duration of the Monitoring Plan to ensure the predicted residual risk for each hazard is achieved (see Section 7.1.2., *Monitoring and Reporting*, for more information). The OPR begins monitoring the safety performance targets as soon as the final Safety Risk Assessment Report, or Addendum if applicable, is signed. Doing so ensures that awareness of the unmitigated risk is maintained during the implementation of the mitigations, which is especially important with those issues having longer term implementation timelines. However, the reporting duration listed in the Monitoring Plan does not begin until all mitigations have been implemented.

There may be instances in which the OPR and HIRMT Program Manager can decide to make a necessary update, such as minor changes to a Monitoring Plan, without the need to fully revisit the safety issue (i.e., reconvene the SRM Team). In those cases, the OPR communicates the change with the appropriate stakeholders and the FAA SMS Committee to ensure that they are aware of the change and justification for the change. However, significant changes that cannot be resolved within the SRM Team or OPR may warrant further interaction with the FAA SMS Committee as described below.

5.2.1. Scenarios Requiring FAA SMS Committee Engagement

When the OPR is unsure whether to escalate a concern to the FAA SMS Committee, they should err on the side of oversharing. The OPR should use the process in Chapter 6, *Escalation of SRM-Related Concerns or Disagreements*, to elevate concerns or disagreements to the FAA SMS Committee. Instances that warrant escalation to the FAA SMS Committee may include, but are not limited to, the situations described below.

5.2.1.1. Missed Safety Performance Target During or After Mitigation Implementation

If a safety performance target is not met during or after mitigation implementation, the OPR, in coordination with the SRM Team as necessary, determines necessary action to address the issue (e.g., re-open or re-work affected mitigations). The OPR would then communicate the necessary action to the FAA SMS Committee and affected Mitigation Owners, along with any modifications to the Monitoring Plan.

5.2.1.2. Change to Related Rule or Regulation

If there is a change to a rule or regulation that could affect the safety issue or assessment findings and/or recommendations, the OPR should determine whether the SRM Team should reconvene to revisit the assessment. Regardless of the need to reconvene, the OPR should notify the FAA SMS Committee of the change in the rule or regulation and report on any necessary action needed by the Team.

5.2.1.3. Changes in OPR or Key Stakeholder Personnel

Changes in OPR organization or personnel within key stakeholder organizations (OPR, Mitigation Owner, etc.) can present challenges with issue coordination. In general, turnover of safety management information should be handled by organizations as they handle turnover of any type of information. Challenges with the turnover/passing on of information due to personnel changes or similar disagreements may be elevated to the FAA SMS Committee.

5.2.1.4. No Safety Recommendations Accepted[23]

There may be Safety Risk Assessments in which none of the safety recommendations from the Safety Risk Assessment Report were accepted by the Mitigation Owners. The OPR should still conduct the activities in the initial Monitoring Plan (or a new Monitoring Plan created by the SRM Team if necessary) to ensure no further negative impact to safety. Note that FAA Order 8040.4 requires monitoring for hazards with medium risk.[23] The OPR should also provide periodic updates to the SCT and/or FAA SMS Committee.

5.3. Step 3: Safety Issue Closure

Once all required mitigations have been implemented and the Monitoring Plan has been carried out (i.e., monitoring activities have been completed through the reporting duration and safety performance targets have been met), the predicted residual risk assessed by the SRM Team is considered verified and is now deemed residual risk. The Issue Status in HIRMT is then changed to “Closed,” and archived for future reference.

OPRs should provide a close out summary which could be as simple as including a close out slide with the regular HIRMT status update at an FAA SMS Committee meeting, with the OPR briefing out on the outcome of the effort and any further steps necessary to ensure the mitigations are achieving the desired result.

Even though the safety issue has been closed out, Safety Assurance processes within the FAA will continue. If an event related to the safety issue occurs after the safety issue has been closed, the OPR should elevate the issue to the FAA SMS Committee again to determine what actions should be taken, including whether SRM should be performed on the issue again.

[23] FAA Order 8040.4 requires that high risk hazards be both mitigated and monitored. Therefore, high risk hazards would not fall into this scenario.

Chapter 6. Escalation of SRM-Related Concerns or Disagreements

FAA Order 8040.4C, Chapter 2, Paragraph 1k, *Safety Risk Management Policy,* states:

> A safety issue may affect multiple LOBs and/or Staff Offices. Under such circumstances, all affected FAA organizations must be part of the process. Effective SRM requires early and ongoing involvement by appropriate members of all affected FAA organizations. If a disagreement arises among FAA organizations regarding SRM that cannot be resolved, the issue should be raised for resolution to the FAA SMS Committee. If a hazard, its associated safety risk, and safety risk controls affect a single LOB or Staff Office, no further coordination beyond that LOB or Staff Office is necessary (except where required by another FAA order).

Based on this requirement in the policy, when the safety issue crosses multiple LOBs, the following process was developed to escalate a concern or disagreement related to SRM to the appropriate levels of FAA and/or LOB/Staff Office management. This process, shown in Figure 6-1, can be used for concerns or disagreements related to an SRM effort sponsored by the FAA SMS Committee or SRM conducted by organizations independent of the FAA SMS Committee, as long as the concern or disagreement meets the criteria in the first step of the escalation process.

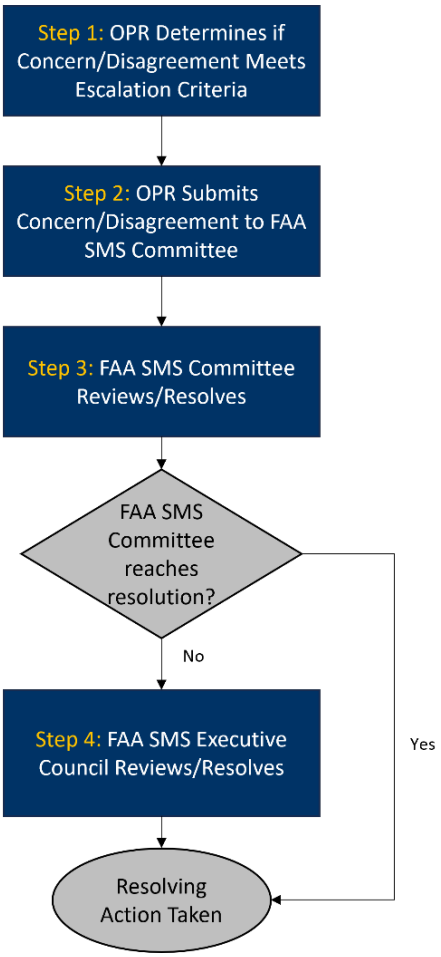


Figure 6-1: Steps to Escalate SRM-Related Concerns or Disagreements

6.1. Step 1: OPR Determines If Concern/Disagreement Meets Escalation Criteria

If there are any disagreements among organizations related to the safety risk assessment before, during, or after the SRM Team meetings, the OPR POC, with assistance from the SRM Facilitation Team if needed, should first determine if the concern or disagreement should be elevated to the FAA SMS Committee. All attempts should be made to resolve the concern or disagreement at the OPR/LOB level; however, there may be times when it needs to be escalated. In order to be escalated, the safety issue needs to meet all four of the following criteria:

1. Crosses multiple FAA LOBs/Staff Offices;
2. Contains hazards that are:
    - High risk, or
    - Medium risk with uncertainty about the risk and/or are based on numerous assumptions;
3. Is an active safety issue (e.g., awaiting response from product/service provider; awaiting results of investigation; gathering further information through an FAA-sponsored study); and
4. Has some disagreement surrounding it that is causing the safety issue to remain unresolved. Some examples are:
    - Disagreement on mitigations;
    - Failure to implement mitigations;
    - Disagreement on the process or methodology used;
    - Disagreement on safety risk assessment;
    - Disagreement as to whether to apply resources; or
    - Disagreement over ownership of hazard and/or controls.

For escalation of concerns that arise during the Monitoring phase of SRM, the OPR should elevate concerns to the FAA SMS Committee using the same methodology as above. Additional criteria or instances that warrant escalation to the FAA SMS Committee may include, but are not limited to, the following examples.

- Missed safety performance target during or after mitigation implementation.
- Change to related a rule or regulation.
- Changes in OPR or key stakeholder personnel.
- No safety recommendations accepted.

6.2. Step 2: OPR Submits Concern/Disagreement to FAA SMS Committee

If the safety issue meets the four criteria in Step 1, the OPR POC works with their representative on the FAA SMS Committee[24] to complete the Safety Issue Concern or Disagreement Escalation Template (see Appendix B, *Templates*), which is submitted to the FAA SMS Committee Chair. For each new concern/disagreement submitted, the FAA SMS Committee Chair reviews the submittal to ensure that it meets the escalation criteria.

6.3. Step 3: FAA SMS Committee Reviews/Resolves

The FAA SMS Committee Chair brings the concern/disagreement to the attention of the FAA SMS Committee. Depending on the urgency of the safety issue, this can be done at a regularly scheduled FAA SMS Committee meeting or at a special meeting called to discuss the concern or disagreement.

[24] See the SMS Contacts page on the FAA Intranet for the list of FAA SMS Committee members,

The OPR POC works with their representative on the FAA SMS Committee and the FAA SMS Committee Chair to make sure that the right SMEs are brought in for the discussions if more information is needed. The FAA SMS Committee discusses the submission with the appropriate experts within the LOBs/Staff Offices to assist in resolving the concern or disagreement. The FAA SMS Committee decides whether the disagreement can be resolved at the FAA SMS Committee level or if it needs to be escalated to the FAA SMS Executive Council. The FAA SMS Committee makes every attempt to resolve the concern or disagreement. If the OPR is not present at the meeting, the FAA SMS Committee Chair notifies the OPR POC of the resolution or decision to escalate further.

6.4. Step 4: FAA SMS Executive Council Reviews/Resolves

If the FAA SMS Committee cannot reach a resolution, the FAA SMS Committee Chair raises the unresolved concern/disagreement to the FAA SMS Executive Council for resolution. Depending on the urgency of the safety issue, this can be done at a regularly scheduled FAA SMS Executive Council meeting or at a special meeting called to discuss the concern or disagreement.

The FAA SMS Committee Chair ensures that the LOBs/Staff Offices involved provide appropriate SMEs needed for discussions at the FAA SMS Executive Council meeting. The FAA SMS Committee Chair communicates the results of the FAA SMS Executive Council meeting with the FAA SMS Committee members and OPR, who in turn share the information with their organizations.

Chapter 7. Hazard Identification, Risk Management and Tracking (HIRMT) System

FAA Order 8040.4, *Safety Risk Management Policy*, describes the purpose and use of the HIRMT system, and provides requirements for documentation of ASL safety issues in HIRMT.

The objectives of HIRMT are to:

- Ensure a uniform method for tracking ASL safety issues across LOBs/Staff Offices based on SRM and Safety Assurance processes described in the current version of FAA Order 8040.4;
- Support the coordination of SRM and Safety Assurance processes across the agency;
- Provide visibility and transparency across LOB/Staff Office areas of responsibility and across disparate complex safety issues;
- Provide a means to monitor implementation of safety risk mitigations/controls and determine whether mitigations produce the expected effect on safety in the aerospace system;
- Improve the agency's ability to identify safety issues most critical to the FAA;
- Enable FAA organizations to better communicate and collaborate with one another on the safety issues that are most critical to the agency;
- Enhance FAA decision making, enabling executives and managers to better focus organizational resources on areas of greatest safety risk; and
- Improve interagency communication and awareness of other agency efforts that may impact data analysis and decision making.

Safety issues that meet ASL safety issue criteria must be documented and reported in HIRMT. The requirements for LOBs and Staff Offices to report ASL safety issues in HIRMT can be found in the current versions of FAA Order 8000.369, *Safety Management System*, and FAA Order 8040.4. Chapter 1, *FAA Safety Issue Identification and Management Process*, of this document describes the criteria for ASL safety issues that must be reported in and managed through HIRMT.

7.1. Managing ASL Safety Issues in HIRMT

The FAA uses HIRMT to manage ASL safety issues from their initial documentation through safety risk assessment and analysis, risk mitigation, and monitoring and tracking effectiveness of mitigations. Entry of information into HIRMT does not stop once the report and addendum are complete. FAA stakeholders report monthly, or another agreed upon frequency, on mitigation and monitoring activities until the safety issue can be closed.

7.1.1. HIRMT Entry for SRM

ASL safety issues that have been identified and approved for agency-level safety risk assessment and tracking are entered into HIRMT by the HIRMT Program Manager within AVP-300 on behalf of the Initiating Organization.

The FAA SMS Committee reviews and tracks safety issues raised through the FAA Safety Issue Identification and Management process described in Chapter 1. As SRM on the safety issue progresses, the OPR provides updates to the HIRMT Program Manager after each SRM step so that the issue status can be updated in HIRMT.

7.1.2. Monitoring and Reporting

After SRM is completed, the Mitigation Owners implement mitigations, and the OPR executes the Monitoring Plan to evaluate whether the safety risk controls that have been employed are achieving their intended objectives and the predicted residual risk is being met.

Mitigation Owners are expected to report monthly, or another agreed upon frequency, on the status of mitigation implementation. The OPR is expected to report on the monitoring activities at the frequency defined in the Monitoring Plan once all mitigations have been implemented. While the reporting duration listed in the Monitoring Plan begins after all approved mitigations have been implemented, monitoring activities should begin as soon as the Safety Risk Assessment Report, or Addendum, if applicable, is signed and entered into HIRMT. If the performance targets are not met, an action plan must be developed and executed to ensure that the targets will be met. Finally, if the mitigations have created new hazards, SRM should be performed to assess the identified hazards. If the Monitoring Plan demonstrates that the system is functioning as expected, the system is deemed in conformance. The HIRMT Program Manager coordinates with the OPR to update HIRMT with information required to perform Safety Assurance functions (monitoring implementation and targets in the Monitoring Plan to ensure mitigations are achieving the expected results). See Chapter 5, *Mitigation Performance Monitoring Process*, for more information on monitoring and reporting.

7.2. HIRMT Dashboard and Mitigation Status Report

AVP-300 developed the HIRMT Dashboard to reflect the results of SRM and the associated Safety Assurance efforts regarding ASL issues, as required by FAA Order 8040.4. The HIRMT Dashboard is comprised of several Tableau dashboards that present the statuses of each mitigation implementation, Monitoring Plan actions, and safety performance target updates. The HIRMT Program Manager coordinates with the appropriate POCs for the various SRM phases to obtain statuses on a monthly basis, or another agreed upon frequency.

The Mitigation Status Report is a live report of open ASL issues and provides an overview of the issues' risks and mitigation statuses. It can be found on the HIRMT Dashboard, which is also accessible from the HIRMT Knowledge Services Network (KSN). The report is presented monthly to the AVSSMS Coordination Group and FAA SMS Committee, and to FAA SMS Executive Council, as appropriate.

7.3. HIRMT KSN

The HIRMT KSN was established as an FAA-wide repository used to store identified ASL and organizational-level aerospace safety issues to include safety hazards, safety risk levels, mitigations, Monitoring Plans, and safety performance targets. The KSN is intended to enable communication and visibility into ASL safety issues across multiple organizations within the FAA. The KSN supports the facilitation and management of the full life cycle of SRM and Safety Assurance efforts. It provides a means to document mitigation implementation and evaluate the effectiveness of those mitigations against performance measures articulated in the safety issue's Monitoring Plan.

The HIRMT Program FAA Intranet site contains links to the HIRMT KSN and HIRMT Dashboard, as well as contact information for the HIRMT Program Manager. The HIRMT KSN is operated and managed as an administrative support system and is not intended to be used by entities outside of the FAA (i.e., only FAA employees and supporting contractors may access the KSN). The HIRMT KSN operates in accordance with FAA Order 8040.4.

7.4. HIRMT Access

HIRMT access is granted to FAA employees or supporting contractors who are expected to perform roles such as monitoring the progress of safety issues entered in HIRMT and/or accessing reports as required by an organization's management.

In compliance with FAA Order 8040.4, the SRM Overview Briefing (eLMS FAA27000023) must be completed prior to requesting access to HIRMT. The training provides a high-level summary of SMS, a review of the ASL safety issue criteria, and a navigation through the SRM/Safety Assurance processes that support HIRMT. Send proof of completion to the HIRMT Program Manager, whose contact information can be found on the HIRMT Program FAA Intranet site, for access to the HIRMT system.

For questions regarding the HIRMT Dashboard, HIRMT KSN, or HIRMT reporting, contact the Safety Policy and Promotion Branch (AVP-320).

Appendix A. Roles and Responsibilities

The aerospace system involves complex interactions between different technical and human centered sub-systems which are operated by many different types of organizations or stakeholders. A stakeholder is a group or individual that is affected by, or is in some way accountable for, the outcome of an undertaking; a stakeholder can also be described as an interested party having a right, share, or claim in a product or service or in its success in possessing qualities that meet that party's needs and/or expectations. Table A-1 provides an overview of the roles and responsibilities of specific Safety Risk Management (SRM) stakeholders in the Federal Aviation Administration (FAA); more specific roles and responsibilities are detailed within the document.

Table A-1: Roles and Responsibilities of Key FAA SRM Stakeholders

Stakeholder	Roles and Responsibilities
FAA Safety Management System (SMS) Executive Council	• Sets the strategic direction for safety management, including SMS and United States (U.S.) State Safety Program (SSP) implementation, across the FAA • Provides executive-level guidance and conflict resolution for FAA safety management-related issues • Meets at regular intervals to exchange safety information and address safety issues • Resolves any issues that the FAA SMS Committee raises, which may include disagreements or requests for additional resources related to SRM activities, Aerospace System Level (ASL) safety issues, and the use of the Hazard Identification, Risk Management & Tracking (HIRMT) system
FAA SMS Committee	• Reports to the FAA SMS Executive Council • Provides assistance to FAA organizations regarding safety management • Meets at regular intervals and at the discretion of the FAA SMS Committee Chair to exchange safety management information • Oversees the development and implementation of the FAA Safety Issue Identification and Management process • Approves, or otherwise addresses, FAA-level safety issues recommended for safety risk assessment • Recommends FAA-level safety issues to the FAA SMS Executive Council for allocation of resources to conduct safety risk assessments, when necessary • Assigns an Office of Primary Responsibility (OPR), if applicable, for assessing and addressing cross-organizational safety issues • Ensures ASL safety issues are reported in HIRMT and approves closure of ASL safety issues within HIRMT • Approves the scope and overarching plan for FAA-level safety risk assessments • Resolves disagreements between FAA organizations regarding safety management, including disagreements related to SRM, ASL safety issues, and the use of HIRMT • Escalates disagreements that cannot be resolved at the FAA SMS Committee level to the FAA SMS Executive Council

Stakeholder	Roles and Responsibilities
Safety Collaboration Team (SCT)	• Establishes teams of Subject Matter Experts (SMEs), stakeholders and facilitators to conduct SRM on safety issues assigned by the FAA SMS Committee • Provides status updates regarding SCT activities to the FAA SMS Committee • Provides SRM consultation and facilitation services for FAA-level safety issues, based on direction from the FAA SMS Committee • Fosters collaboration supporting the advancement and common understanding of cross-organizational SRM among safety professionals
Office of Accident Investigation and Prevention, Safety Management Division (AVP-300)	• Manages the FAA SMS and its supporting policies, processes, and tools in support of the Associate Administrator for Aviation Safety (AVS-1), the FAA SMS Executive Council, and the FAA SMS Committee • Chairs the FAA SMS Committee • Develops FAA-wide safety management policy and supporting safety management guidance • Manages the identification of cross-organizational safety issues at the FAA level on behalf of the FAA SMS Committee • Coordinates safety risk assessment efforts for FAA-level safety issues, tracks approved safety risk mitigations, and measures safety performance for the FAA • Ensures that the FAA-level safety risk assessment activities are managed through the SRM/Safety Assurance processes on behalf of the FAA • Manages HIRMT, as well as supporting policies, processes, guidance materials, and the HIRMT Knowledge Services Network (KSN) • Manages the use of HIRMT for ASL safety issues, which includes entering information from SRM documentation, monitoring the implementation status of mitigations, and producing reports for FAA executive management to facilitate communication and accountability regarding ASL safety issues • Performs the HIRMT oversight functions; ensures compliance with FAA Order 8040.4 requirements • Provides assistance/expertise to FAA organizations regarding safety risk management and tracking hazards in HIRMT
Initiating Organization	• Identifies a safety issue and raises it to the FAA SMS Committee for support to conduct a cross-Line of Business (LOB) safety risk assessment (Note: Organizations can establish SRM Teams without engaging the FAA SMS Committee for non-ASL issues. However, the FAA SMS Committee is a resource to facilitate the coordination of the assessment and the establishment of an SRM Team, particularly for those that are cross-LOB.) • Coordinates with the HIRMT Program Manager within AVP-300 to have the safety issue entered into HIRMT, in accordance with the FAA Safety Issue Identification and Management process • May or may not be the OPR for the safety risk assessment

Stakeholder	Roles and Responsibilities
Office of Primary Responsibility (OPR)	• Responsible for managing and tracking the safety issue through closure • Leads and manages the safety risk assessment and presents findings and recommendations to decision makers • Confers with the Office of the Chief Counsel (AGC) in cases where SME participation from non-governmental entities is necessary on the SRM Team in order to avoid any potential data protection and/or legal/statutory issues, as well as ensure conformance with Freedom of Information Act (FOIA) requirements • Ensures accuracy of the technical information entered into HIRMT and provides status updates to the HIRMT Program Manager for entry into HIRMT based on the Monitoring Plan through closure of the safety issue • Identifies the appropriate management officials to accept safety risk and approve mitigations • Coordinates any necessary approvals and safety risk acceptance decisions, and provides them to the HIRMT Program Manager to ensure that results and decisions are captured in HIRMT on behalf of the risk acceptance or approval authorities • Provides status updates to the FAA SMS Committee and SCT • Includes two main roles—the OPR Manager and the OPR Point of Contact (POC) • Appropriate management official within the OPR selects the OPR Manager
OPR Manager	• Decision maker within the OPR that has the biggest stake in the safety issue • Accepts/rejects the role as OPR on behalf of the responsible organization • Confirms management designation of OPR POC • Approves assessment scope and draft system analysis for safety risk assessments • Assists the OPR POC with identification of the Risk Accepter and Mitigation Owner, as needed • Approves the final Safety Risk Assessment Report and Addendum via signature • Approves the Monitoring Plan
OPR Point of Contact (POC)	• Assists the SRM Facilitation Team to complete and document the safety risk assessment effort • In coordination with the HIRMT Program Manager, documents SRM and Safety Assurance status updates and results in HIRMT • Identifies the Risk Accepter and Mitigation Owners (with OPR Manager assistance as needed) • Ensures that the assessment scope and system analysis developed by the SRM Team is accurate • Ensures that the SRM Team developed the Safety Risk Assessment Report properly, systematically identified hazards, and assessed the safety risk appropriately • Works with the appropriate management official(s) to ensure that the SRM Team proposed appropriate and practical safety risk mitigations, as well as an appropriate and practical Monitoring Plan

Stakeholder	Roles and Responsibilities
OPR POC (continued)	• Agrees to follow and execute a comprehensive Monitoring Plan to verify the predicted residual risk; provides information to the HIRMT Program Manager for documentation in HIRMT • With help from the SCT and Facilitation Team, acquires signatures for safety risk mitigation approvals and safety risk acceptance, following existing organizational processes for approvals and acceptances, as appropriate • Briefs the activities pertaining to their assigned ASL safety issue to management, as needed • Engages with the appropriate management and stakeholders within their respective organization to maintain transparency of the safety issue and its status • Initiates the request to close an ASL safety issue in HIRMT • Uses the Process for Escalation of SRM-Related Concerns or Disagreements (see Chapter 6) to escalate the concern if any disagreements among organizations related to the assessment occur before, during, or after the SRM Team meets
SRM Team Member	• Participates within a diverse group of representatives, stakeholders, and SMEs from the various organizations affected by the safety issue[25] • Examines potential safety risk of the safety issue and the causes of that risk • Conducts SRM on the safety issue in accordance with the current version of FAA Order 8040.4 • Determines the appropriate breadth and depth of the safety analysis based on the presence of, or potential for, hazards and safety risk • Objectively assesses the safety risk of the safety issue • If some decisions in the assessment must be put to a vote, only one SRM Team member per organization should be given authority to vote on behalf of their organization • Conducts additional data searches as needed to complete a thorough safety risk assessment • Documents the Team's safety findings in a Safety Risk Assessment Report as an input to decision making • Develops the Safety Risk Assessment Report Addendum to attach to the Safety Risk Assessment Report • May help the SRM Team Facilitator and OPR POC obtain safety recommendations approval • Engages with appropriate management and stakeholders within their respective organization to maintain transparency of the safety issue and its status • Reviews the FAA SRM Overview Briefing (FAA27000023) prior to attending their first SRM Team meeting

[25] The SRM Team may include stakeholders external to the FAA. Section 2.3, *Determine and Secure SRM Team Members*, in Chapter 2 provides more information regarding external stakeholders.

Stakeholder	Roles and Responsibilities
SRM Team Observer	• Attends meetings because they have particular knowledge or experience related to the safety issue being assessed or they are trying to gain experience with the SRM process • Does not participate in SRM Team member discussions or decisions, unless specifically called upon by the SRM Team to contribute • Does not participate in Safety Risk Assessment Report or Addendum reviews or provide comments regarding the report or addendum
SRM Team Facilitator(s)	• Along with the Documentation Analyst, comprises the Facilitation Team • Has received sufficient training on SRM and facilitation to perform facilitator duties • Works with the OPR to help scope the safety risk assessment and moderate SRM Team deliberations • Works with the OPR and FAA SMS Committee Chair to prepare and distribute the Resource Request Memo before the SRM Team convenes • Requests briefings and collects all available and relevant safety information regarding the safety issue, as necessary, before the SRM Team convenes • Provides all relevant information about the safety issue to SRM Team members prior to the SRM Team Kickoff Meeting • Notifies all identified SRM Team members of meetings and coordinates logistics for the meetings • Ensures the SRM Team complies with the SRM process • Limits their influence on the safety risk assessment • Guides participants in objectively examining and identifying potential safety hazards and mitigating the safety risk associated with those hazards • Engages the Team to develop a thorough safety risk assessment by soliciting expert advice and building consensus whenever possible • Cultivates discussion among Team members about potential hazards, risks, and mitigations • Performs or delegates the functions of timekeeper to manage start times and breaks • Coordinates review of the Safety Risk Assessment Report and Addendum within the SRM Team and delivers the final report and addendum to the OPR • Works with the SCT Co-Chairs to coordinate a peer review of the Safety Risk Assessment Report and Safety Risk Assessment Report Addendum • Mediates and assists SRM Team members in working through differences of opinion • Remains neutral to the outcome

Stakeholder	Roles and Responsibilities
Documentation Analyst	• Along with the SRM Team Facilitator(s), comprises the Facilitation Team • Documents SRM Team findings and proposed safety risk mitigation strategies • Assists the SRM Team with writing the Safety Risk Assessment Report and Addendum • Develops the necessary reports and communication materials to deliver the results to management • Assists the SRM Team Facilitator(s), as needed, during all phases of conducting the safety risk assessment
Various Safety Management Professionals	• Typically assigned to support large/complex SRM/Safety Assurance efforts • Monitor SRM efforts for individual ASL safety issues within HIRMT • Monitor their organization's SRM performance within HIRMT • Monitor ASL safety issues in which their organization has a stake • Report status of ASL safety issues and mitigations up their management chain
HIRMT Program Manager (resides within AVP-300)	• Enters the safety issue and SRM information into HIRMT on behalf of, and in coordination with, the OPR • Monitors the progression of ASL safety issues through the SRM/Safety Assurance process and ensures that FAA Order 8040.4 requirements are met • Provides HIRMT user community support in conducting SRM/Safety Assurance, as needed • Provides ASL safety issue status updates and reports to the FAA SMS Committee and FAA executive management on a quarterly basis and when requested • Approves closure of ASL safety issue requests on behalf of the FAA SMS Committee
Risk Accepter[26]	• Based on the safety risk assessment, decides whether to accept the risk • Signs a memo affirming any decisions made and confirming risk acceptance (Note: The signature is for documentation/record purposes only. Risk acceptance for safety issues can occur regardless of the signature status. Planned changes cannot proceed without a risk acceptance signature.)
Mitigation Owner	• Accepts responsibility for implementing and monitoring the mitigation • Provides approval signature in the Safety Recommendation Approvals document, representing commitment to implement the safety risk mitigation as documented • Provides plan for implementation and expected implementation date for each mitigation upon signature approving the mitigation • Provides mitigation and monitoring status updates to the HIRMT Program Manager on a monthly basis, or other agreed upon frequency

[26] The person authorized to accept risk on behalf of the organization varies based on the level of risk being accepted. Refer to Table 2-1: Safety Risk Acceptance Criteria for Issues or Changes That Cross LOBs/Staff Offices, in the current version of FAA Order 8040.4 for the level of management that can accept risk.

Stakeholder	Roles and Responsibilities
Monitoring Plan Data Owner	• As designated by the OPR and SRM Team, collects specific data items from the agreed-upon data source/database identified in the Monitoring Plan, throughout the duration of the Monitoring Plan. (Note: The Monitoring Plan Data Owner may be different from the organization responsible for analyzing the data and determining safety performance.) • Reviews the proposed Monitoring Plan and provides feedback to the OPR and SRM Team on whether the identified data can feasibly be collected

Appendix B. Templates

Table B-1 shows the templates and resources for use throughout the cross-Line of Business (LOB) safety risk assessment process. Following the table, there is a brief description of each template and a hyperlink to its location on the Federal Aviation Administration (FAA) Intranet.

Table B-1: Templates and Resources for the FAA Safety Issue Identification and Management Process and Cross-LOB Safety Risk Assessments

Step	Template/Resource
FAA Safety Issue Identification and Management Process	
Step 1: Identify Potential Safety Issue	• Section 1.1 in Chapter 1: FAA Safety Issue Identification and Management Process
Step 2: Conduct Preliminary Safety Risk Assessment	• Preliminary Safety Risk Assessment Template
Step 3: Enter Safety Issue in the Hazard Identification, Risk Management and Tracking (HIRMT) system	• Chapter 7: Hazard Identification, Risk Management and Tracking (HIRMT) System
Step 4: Apply Criteria for Elevating to FAA SMS Committee	• Section 1.2.4 in Chapter 1: FAA Safety Issue Identification and Management Process
Step 5: Request Cross-LOB Safety Risk Assessment Team	• Request for FAA SMS Committee Action Briefing Template
Step 6: FAA SMS Executive Council Reviews/Resolves	N/A
Planning Cross-LOB Safety Risk Assessments	
Conduct Initial Planning	• Issue Summary Template
Establish Scope and Draft System Analysis	• Issue Summary Template
Determine and Secure Safety Risk Management (SRM) Team Members	• Resource Request Memo Template • External Stakeholder Resource Request Template
Ensure Management Awareness of Team Membership	N/A
Develop Detailed Schedule and Communicate with SRM Team	• Issue Summary Template • SRM Team Kickoff Briefing Template
Conducting the SRM Process	
Conduct SRM	• Chapter 3: Conducting the SRM Process • Appendix C: SRM Tools • Hazard Analysis Worksheet (HAW) Template

Step	Template/Resource
Documenting Cross LOB Safety Risk Assessments and Obtaining Mitigation Approvals	
Draft and Review Safety Risk Assessment Report	• Safety Risk Assessment Report Template • Comment Matrix Template • Record of Comments and Other Opinions Template
Finalize Safety Risk Assessment Report	• Safety Risk Assessment Report Signature Memo Template • Safety Issue Status Briefing Template
Obtain Approval of Safety Mitigations	• Safety Recommendation Approvals Template
Risk Acceptance	• Risk Acceptance Memo Template
Reassess Predicted Residual Risk and Develop Safety Risk Assessment Report Addendum	• Safety Risk Assessment Report Addendum Template • Safety Risk Assessment Report Addendum Signature Memo Template
Monitor Mitigations and Report Status	• Safety Issue Status Briefing Template
Escalation of SRM-Related Concerns or Disagreements	
Escalate SRM-Related Concerns or Disagreements, if necessary	• Chapter 6: Escalation of SRM-Related Concerns or Disagreements • Safety Issue Concern or Disagreement Escalation Template

B.1. Preliminary Safety Risk Assessment Template

Once a safety issue has been identified, the Initiating Organization (or the Office of Accident Investigation and Prevention [AVP] for safety issues identified through the Issue Identification Function) conducts a preliminary safety risk assessment utilizing the Preliminary Safety Risk Assessment Template. The template includes a description of the safety issue, background, stakeholders, hazards, and risk levels. The preliminary assessment does not need to be complex; it is intended to support decision makers in determining whether to direct resources toward a more detailed and complete analysis of the safety issue. Download: Preliminary Safety Risk Assessment Template.

B.2. Request for FAA SMS Committee Action Briefing Template

The Initiating Organization uses this template to brief and request that the FAA SMS Committee provide cross-organizational resources to form an SRM Team to assess a safety issue. Briefing template sections include Description of Issue, Stakeholders, Summary of Safety Assessments Conducted to Date, Preliminary Safety Risk Assessment and Assessment of Impact, Preliminary Hazards, and Recommendation to FAA SMS Committee. Download: FAA SMS Committee Action Briefing Template.

B.3. Issue Summary Template

Initial planning is necessary to conduct SRM. Using this template, the Office of Primary Responsibility (OPR) Point of Contact (POC) articulates what the SRM Team is trying to accomplish and defines an assessment timeline in order to communicate a high-level plan to stakeholders/potential SRM Team members. Template sections include Topic Overview, What

is Happening, What We Have Done to Date, Next Steps, Draft 5M Model, Stakeholders, Draft Preliminary Hazard List, and Draft Timeline. Download: Issue Summary Template.

B.4. Resource Request Memo Template

SRM Teams should include representatives from the various organizations affected by the safety issue. It is important that the Team be diverse and include stakeholders and experts who are expected to be involved in various capacities throughout the SRM process. The OPR POC identifies the skills and expertise required to conduct the safety risk assessment and then formally requests Team member participation with this template. Download: Resource Request Memo Template.

B.5. External Stakeholder Resource Request Template

Sometimes an SRM Team needs expertise from subject matter experts (SMEs) outside the FAA. In that case, the OPR POC requests participation using this template. Note that the OPR must also confer with the Office of the Chief Counsel (AGC) to avoid any potential data protection and/or legal/statutory issues, as well as comply with any Freedom of Information Act (FOIA) requirements. Download: External Stakeholder Resource Request Template.

B.6. SRM Team Kickoff Briefing Template

This template is for the SRM Team Kickoff meeting. The OPR POC and the SRM Team Facilitator(s) brief Team members on Team objectives, a background on the safety issue, the overall FAA SRM Process, ground rules, and how the Team will conduct its assessment. Download: SRM Team Kickoff Briefing Template.

B.7. Hazard Analysis Worksheet (HAW) Template

The SRM Team completes all five SRM steps using the Hazard Analysis Worksheet (HAW) Template. The template includes sections to Analyze System, Identify Hazards, Analyze Safety Risk, Assess Safety Risk, and Control Safety Risk. Download: HAW Template.

B.8. Safety Risk Assessment Report Template

The SRM Team, SRM Team Facilitator, and the Documentation Analyst use this template to document the Team's safety risk assessment results. The report will detail all five steps of the SRM Process, as well as the Team’s rationale. Download: Safety Risk Assessment Report Template.

B.9. Comment Matrix Template

The SRM Team uses this template to review and submit comments on the draft Safety Risk Assessment Report and the Safety Risk Assessment Report Addendum, if applicable. The OPR POC leads a sub-team to resolve Team comments, which are provided back to the commenters. Download: Comment Matrix Template.

B.10. Record of Comments and Other Opinions Template

There may be instances in which not all SRM Team members agree on the results of the safety risk assessment. This template is used to document comments and other opinions, which become an appendix to the Safety Risk Assessment Report. Download: Record of Comments and Other Opinions Template.

B.11. Safety Risk Assessment Report Signature Memo Template

This template is used to approve the Safety Risk Assessment Report. Approval means that the OPR Manager signs the memo accompanying the report, indicating agreement that the findings are valid and accurate, and that the process was followed. Peer reviewers also sign the memo

to indicate that the report was developed properly and the risk was appropriately assessed. Download: Safety Risk Assessment Report Signature Memo Template.

B.12. Safety Issue Status Briefing Template

As needed, the OPR provides status updates to management and the FAA SMS Committee using this template. Briefing template sections include Overview, Background, SRM Team Meeting Information, SRM Team Members, SRM Team Objective, Hazard Summary, Safety Recommendations/Requirements, Next Steps, and Timeline. Download: Safety Issue Status Briefing Template.

B.13. Safety Recommendation Approvals Template

This template is used to document Mitigation Owners' approval, modification, or rejection of the safety recommendations developed by the SRM Team. The OPR, with help from the Facilitation Team, develops the Safety Recommendation Approvals document and delivers it to the Mitigation Owners once the Safety Risk Assessment Report is approved. Mitigation Owners will indicate whether the recommendation is accepted, provide an expected implementation date, designate a POC for the mitigation, and provide a signature confirming their answers. Any recommendations that are accepted are converted to safety requirements upon signature. Note that this template is read-only due to the importance of accurately creating the form fields. Reach out to the Safety Risk Management and Safety Assurance Branch (AVP-310) for assistance on creating this document. Download: Safety Recommendation Approvals Template.

B.14. Risk Acceptance Memo Template

In order to document risk acceptance, the Risk Accepter will sign a memo describing the safety issue, risk level, and any decisions that were made. However, the signature is for documentation/record purposes only. Risk acceptance for safety issues occurs regardless of the signature status. Planned changes cannot proceed without a risk acceptance signature. Download: Risk Acceptance Memo Template.

B.15. Safety Risk Assessment Report Addendum Template

This template is used to document any changes to the predicted residual risk or Monitoring Plan based on the approved safety requirements. If any of the safety recommendations were modified or rejected, the SRM Team will reconvene to determine whether the predicted residual risk changes based on the mitigations that will be implemented. The SRM Team also either develops, modifies, or confirms the Monitoring Plan. Download: Safety Risk Assessment Report Addendum Template.

B.16. Safety Risk Assessment Report Addendum Signature Memo Template

This template is attached to the Safety Risk Assessment Report Addendum. Signatures from the OPR Manager and peer reviewer(s) on the memo indicate that the Safety Risk Assessment Report Addendum was developed properly, and the safety risk was appropriately assessed. There is also agreement that the findings are valid and accurate, and the process was followed. Download: Safety Risk Assessment Report Addendum Signature Memo.

B.17. Safety Issue Concern or Disagreement Escalation Template

If there are any disagreements among organizations related to the safety risk assessment before, during, or after the SRM Team meetings, the OPR POC should first determine if the issue should be elevated to the FAA SMS Committee. If so, the OPR POC works with their representative on the FAA SMS Committee to complete this template and escalate the issue. Download: Safety Issue Concern or Disagreement Escalation Template.

Appendix C. SRM Tools

While the Lines of Business (LOBs) agree on the five basic steps of Safety Risk Management (SRM), the methodologies and tools in performing SRM can differ from one organization to another. Federal Aviation Administration (FAA) Order 8040.4, *Safety Risk Management Policy*, provides a common methodology, including severity and likelihood definitions and risk matrices, which can be used when an SRM project crosses LOBs. This does not preclude an LOB from using its own methodologies in addition to or as part of this common methodology. They can then present this material to the SRM Team as supporting information. It is important that LOBs recognize the differences in how SRM is conducted (and the reasons why it is done so) in order to keep an open mind when viewing the information. The materials will provide substantive information for a robust dialogue amongst the Team.

C.1. System Analysis Tools

The following table provides a summary of the System Analysis tools described in this document.

Table C-1: System Analysis Tools

Tool or Technique	Summary Description
5M Model	The 5M Model is used to capture the information needed to bound and describe the system and aid in the hazard identification process. The components of the 5M Model are: Mission, huMan, Machine, Management, and Media.
SHELL Model	The SHELL model is named after the initial letters of its components (software, hardware, environment, liveware) and places emphasis on the human being and human interfaces with other components of the aviation system.

C.1.1. 5M Model

OVERVIEW: The 5M Model is one useful method to capture the information needed to describe the system. The 5M Model illustrates five integrated elements in any system. As applied to the aerospace system, elements of the 5M Model are:

- **Mission** – A clear and concise description of the safety issue or planned change that the SRM Team was tasked to assess
- **(hu)Man/person** – The human operators, maintainers, and affected stakeholders; stakeholders include those exposed to harm/damage, as well as both internal and external organizations
- **Machine** – The equipment used in the system including, but not limited to, hardware, firmware, software, human-to-system interfaces, system-to-system interfaces, and avionics
- **Management** – The procedures and policies that govern the system's behavior
- **Media** – The environment in which the system is operated and maintained (i.e., the elements of the National Airspace System [NAS] that are affected by the issue or change)

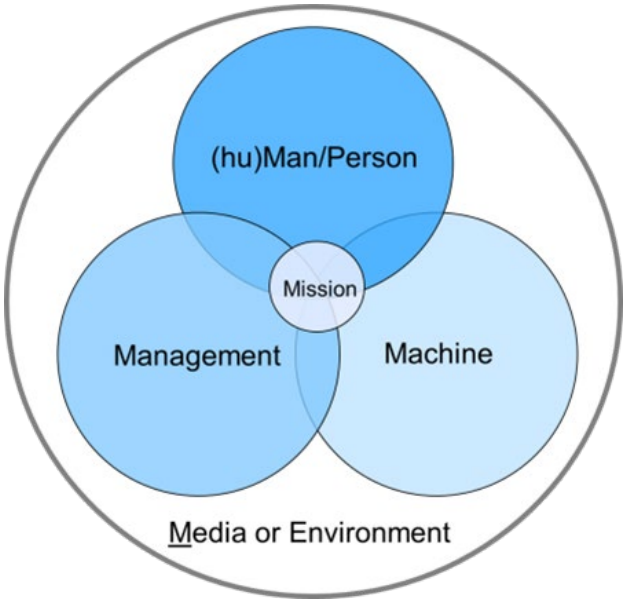


Figure C-1: 5M Model

The 5M Model is used 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.

C.1.2. SHELL Model

OVERVIEW: The SHELL model is named after the initial letters of its components (software, hardware, environment, liveware)[27] and places emphasis on the human being and human interfaces with other components of the aviation system. In the SHELL model, the match or mismatch of the blocks (interface) is just as important as the characteristics described by the blocks themselves. These blocks may be re-arranged as required to analyze and describe the system. A connection between blocks indicates an interface between the two elements.

Each element of the system should be described both functionally and physically if possible. A function is defined as:

> *An action or purpose for which a system, sub-system, or element is designed to perform.*

The functional description should describe what the system is intended to do and should include sub-system functions as they relate to and support the system function.

The physical description provides the audience with information regarding the real composition and organization of the tangible system elements. The level of detail varies with the size and complexity of the system, with the end objective being adequate audience understanding of the safety risk.

[27]Liveware refers to the human beings—the controller with other controllers, flight crews, engineers and maintenance personnel, management, and administration people—within the system.

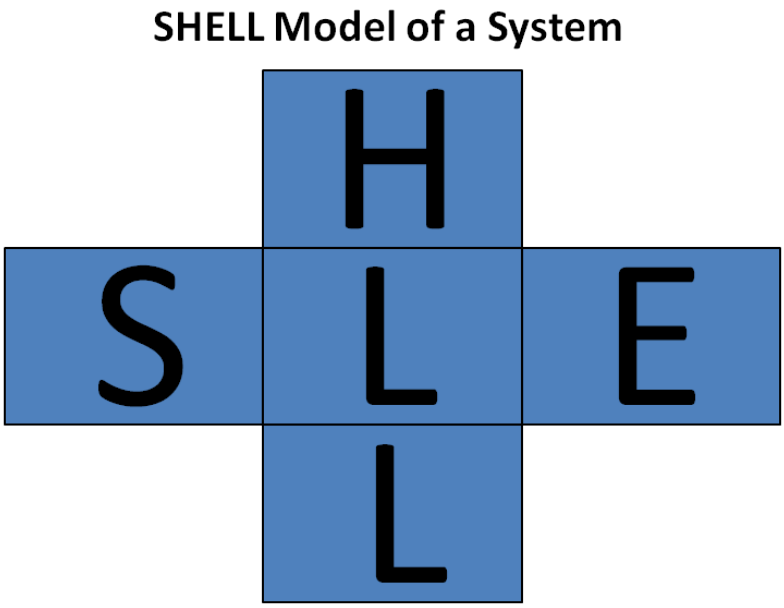


Figure C-2: SHELL Model

C.2. Identify Hazards and Analyze Risk Tools

The following are important considerations to account for when selecting hazard identification/ analysis tools:

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

The tools described in this section are just some of the choices that SRM Teams can consider in their analytical activities. The choice should be made by considering the complexity of the safety issue or planned change being addressed in the course of SRM. Some methods are simple and others more robust in handling complexity. The choice should also consider the ease and clarity of problem understanding within the SRM Team and Office of Primary Responsibility (OPR). The choice should consider other similar efforts and the need for an apples-to-apples comparison result. A fresh look at the problem might have value, but if the results cannot be faithfully repeated, dissention may be the unwelcome result. In many cases,

using a single tool or technique will suffice. Some cases, however, may require multiple tools and techniques. Whomever performs the hazard analysis selects the tool that is most appropriate for the type of system being evaluated.

The following table depicts a selection of hazard identification and analysis tools and techniques that can be helpful in identifying and analyzing hazards. More tools are available on the FAA Acquisition System Toolset (FAST) website.

Table C-2: Identify Hazards and Analyze Risk Tools and Techniques

Tool or Technique	Summary Description
Bow-Tie Model	The Bow-Tie model is a structured approach in which causes of hazards are directly linked to possible outcomes or effects in a single diagram.
Cause and Effect Tool	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.
Change Analysis	The Change Analysis is intended to be used 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, just 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.
Common Cause Failure Analysis (CCFA)	The CCFA is an extension of the Fault Tree Analysis and is used to identify "coupling factors" that can cause component failures to be potentially interdependent.
Comparative Safety Assessment (CSA)	The CSA is used to provide management with a listing of all the hazards associated with a change, along with a risk assessment for each alternative hazard combination that is considered. It considers if each alternative has acceptable safety risk. The CSA's broad scope is an excellent way to identify issues that may require the use of more detailed hazard identification tools.
Crow-AMSAA Reliability Growth Model	Crow-AMSAA is an analytical technique that is used to model event data and forecast the number and timing of future occurrences of those events.
Energy Trace Analysis (ETA)	This hazard analysis approach is used to address all sources of uncontrolled and controlled energy that have the potential to cause an accident.
Energy Trace and Barrier Analysis (ETBA)	The ETBA is a procedure intended to be used 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.
Expected Value Tool	The Expected Value Tool is an Excel-based tool that automatically converts the FAA 8040.4C likelihood definitions into expected value definitions based on an assigned exposure.

Tool or Technique	Summary Description
Failure Mode and Effects Analysis (FMEA)	The FMEA is used to determine the results or effects of sub-element failures on a system operation and classify each potential failure according to its severity.
Failure Modes, Effects, and Criticality Analysis (FMECA)	The FMECA is used to identify component and sub-system failure modes (including the impact of human error); evaluate the results of the failure modes; determine rates and probability; and demonstrate compliance with safety requirements. The FMECA is an essential function in design from concept through development. To be effective, the FMECA is iterative to correspond with the nature of the design process itself.
Fault Hazard Analysis (FHA)	The FHA is a deductive method of analysis that can be used exclusively as a qualitative analysis or, if desired, can expand to a quantitative one. The FHA requires a detailed investigation of the sub-systems to determine component hazard modes, causes of these hazards, and resultant effects on the sub-system and its operation.
Fault Tree Analysis (FTA)	An FTA is a graphical design technique that can be used as an alternative to block diagrams. It is a top-down, deductive approach structured in terms of events. It is used to model faults in terms of failures, anomalies, malfunctions, and human errors.
Hazard Analysis Worksheet (HAW)	The HAW is a worksheet used to document a safety analysis. Using the HAW helps SRM Teams overcome the tendency to focus on safety risk in one aspect of an operation and overlook more serious issues elsewhere in the operation. Its broad scope guides the identification of issues that may require analysis with more detailed hazard identification tools.
Hazard Enterprise Assessment Tool (HEAT)	HEAT is a decision-support tool that provides a structured, data-driven methodology for SRM assessments. It identifies areas in safety risk assessments that require subject matter expert (SME) knowledge and utilizes their qualitative input in conjunction with quantitative safety data drawn from the National Transportation Safety Board (NTSB) aviation accident database and Accident and Incident Data System (AIDS).
The Hazard and Operability Tool (HAZOP)	The special role of the HAZOP is hazard analysis 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.
Interface Analysis	The Interface Analysis is intended to be used to uncover the hazardous linkages or interfaces between 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 looking at these potential energy transfers between two different activities, we can often detect hazards that are difficult to detect in any other way.
Interview Tool	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. The purpose of the Interview Tool is to capture the experience of these personnel in ways that are efficient and positive for them. Properly implemented, the Interview Tool can be among the most valuable hazard identification tools.
Job Hazard Analysis (JHA)	The purpose of the JHA is to examine in detail the safety considerations of a single job. A variation of the JHA, called a task analysis, focuses on a single task, i.e., some smaller segment of a "job."

Tool or Technique	Summary Description
Job Task Analysis (JTA)	The foundation of the performance of a Human Error Analysis (HEA) is a JTA, which is used to describe each human task and sub-task within a system in terms of the perceptual (information intake), cognitive (information processing and decision making), and manual (motor) behaviors required of an operator, maintainer, or support person. The JTA should also be used to identify: the skills and information required to complete tasks, equipment requirements, the task setting, time and accuracy requirements, and the probable human errors and consequences relating to these areas. There are several tools and techniques for performing task analyses, depending on the level of analysis needed.
Logic Diagram	The Logic Diagram is intended to provide considerable structure and detail as a primary hazard identification procedure. Its graphic structure is an excellent means for capturing and correlating the hazard data produced by the 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. An important purpose of the Logic Diagram is to establish the connectivity and linkages that often exist between hazards. It does this very effectively through its tree-like structure.
Management Oversight and Risk Tree (MORT)	The 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 that might be present in an operation. The MORT diagram is very effective in assuring attention to the underlying management root causes of hazards.
Mapping Tool	The map analysis is designed to use terrain maps and other system models and schematics to identify both things at risk and the sources of hazards.
Monte Carlo Simulation	The Monte Carlo simulation uses repeated random sampling to estimate the expected number of future events (expected outcome) for specific problems as a function of specific operational and maintenance constraints.
Multi-Linear Events Sequencing Tool (MES)	The MES tool is a specialized hazard identification procedure designed to detect hazards arising from the time relationship of various operational activities. The MES tool is used to detect situations in which either the absolute or relative timing of events may create risk. The MES tool can be used as a hazard identification tool or as an incident investigation tool.
Operating and Support Hazard Analysis (O&SHA)	The O&SHA is performed primarily to identify and evaluate the hazards associated with the environment, personnel, procedures, operation, support, and equipment involved throughout the total life cycle of a system/element.
Operational Safety Assessment (OSA)	The OSA is a development tool based on the assessment of hazard severity. It establishes safety objectives and safety requirements to meet those objectives. It then subsequently allocates them between air and ground components and determines how performance and interoperability requirements might be influenced. The OSA includes three elements: (1) The Operational Services and Environment Description (OSED) (2) An Operational Hazard Assessment (OHA) (3) An Allocation of Safety Objectives and Requirements (ASOR)

Tool or Technique	Summary Description
Operations Analysis (OA)	The OA provides 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 a major weakness of traditional risk management, which tends to focus effort 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.
Poisson Distribution	The Poisson distribution is used to model data that occurs as discrete events within a given period of time or distance.
Preliminary Hazard Analysis (PHA)	In acquisitions, the PHA is an initial effort to document the risk assessment of the selected system or change.
Preliminary Hazard List (PHL)	The PHL is a hazard identification tool used to list all potential hazards in the overall operation. Development of a PHL typically begins with a brainstorming session among the individuals performing the safety analysis.
Root Cause Analysis (RCA)	The RCA is a method of problem solving that is designed to be applied after an incident as a means to identify systemic root causes that can be mitigated or eliminated from recurring. Though it uses reactive data collection methods, it is actually a proactive prevention technique. RCA is basically a step-by-step process for how to use the Fault Tree Analysis.
Scenario Process Tool	The Scenario Process tool is used to identify and correct potentially hazardous situations by postulating accident scenarios in cases where it is credible and physically logical to do so.
Sneak Circuit Analysis (SCA)	The SCA is a unique method of evaluating electrical circuits. SCA employs recognition of topological patterns that are characteristic of all circuits and systems. The purpose of this analysis technique is to uncover latent (sneak) circuits and conditions that inhibit desired functions or cause undesired functions to occur, without a component having failed.
Subsystem Hazard Analysis (SSHA)	In acquisitions, the general purpose of the SSHA is to perform a safety risk assessment of a system's sub-systems and components at a more detailed level than that provided in a Preliminary Hazard Analysis.
System Hazard Analysis (SHA)	In acquisitions, the general purpose of the SHA is to perform a detailed safety risk assessment of a system, in particular, the interfaces of that system with other systems and the interfaces between the sub-systems that compose the system under study. The SHA and Subsystem Hazard Analysis are interrelated analyses that may be done concurrently.
System-Theoretic Process Analysis (STPA)	STPA is a hazard analysis technique for complex systems based on systems theory. It is a proactive evolution of the System Theoretic Accident Model and Processes (STAMP) accident causality model.
Weibull Distribution	The Weibull distribution is commonly used to model event data. The main advantages of the Weibull distribution are that it can model a variety of data, it handles suspensions (non-event points) easily, and it provides a simple graphical solution and description of the data.
"What If" Tool	The "What If" tool is one of the most powerful hazard identification tools. As in the case of the Scenario Process tool, 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. Because of its ease of use, it is probably the single most practical and effective tool for use by operational personnel.

Contact the SRM Point of Contact in your organization for more information on these and other tools.

C.2.1. Bow-Tie Model

OVERVIEW: The Bow-Tie model is a structured approach in which causes of hazards are directly linked to possible outcomes or effects in a single diagram. This model assumes each hazard can be represented by one or many causes, having the potential to lead to one or many outcomes/effects in various system states. The underlying analysis can be simple or complex depending on what is appropriate for the change being analyzed.

MODEL STRUCTURE: The Bow-Tie model that follows illustrates the relationship between causes, hazards, and what kind of environment (system state) enables their propagation into the different outcomes/effects. This model assumes each hazard can be represented by one or many causes, having the potential to lead to one or many outcomes/effects in various system states.

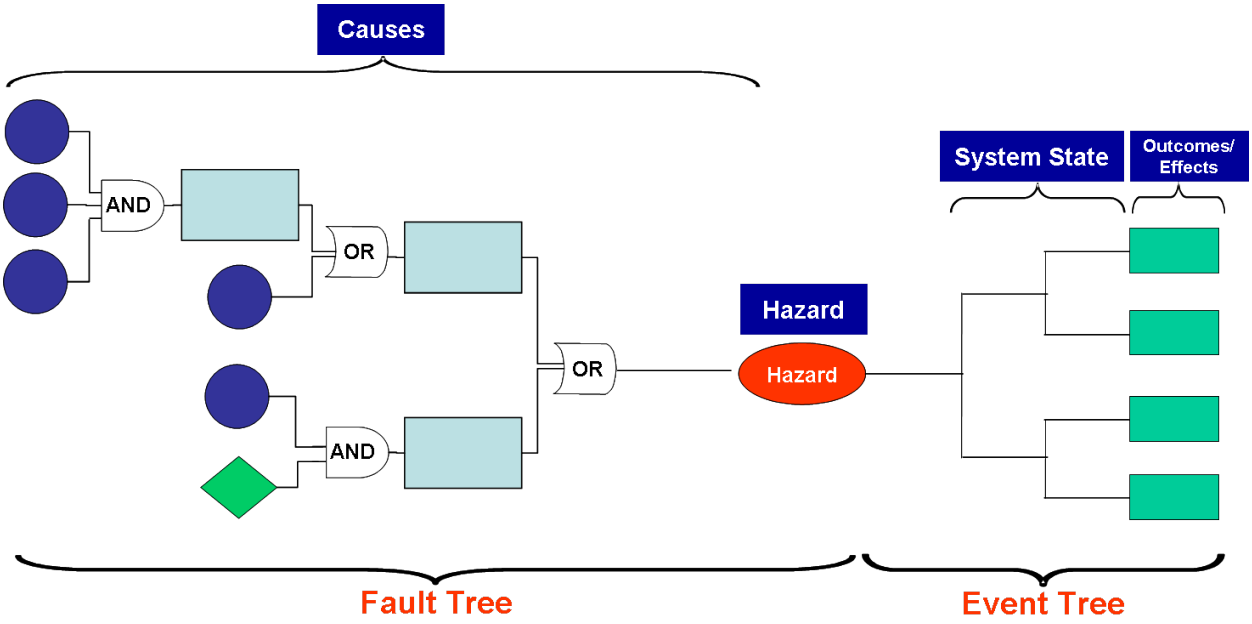


Figure C-3: Bow-Tie Model

For each outcome/effect associated with the hazard, one assigns a severity. To understand a hazard's severity, one determines the hazard's cause and the circumstances under which it occurred (e.g., the system state). The same model can be used to help determine the likelihoods associated with the different outcomes/effects that are the result of a particular hazard given the outlined system states.

C.2.2. Cause and Effect Tool

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

PURPOSE: The Cause and Effect Tool is a variation of the Logic Diagram. The particular advantage of the Cause and Effect Tool is its origin in the quality management process and the numerous personnel who have been trained in the tool. Because it is widely used, many 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 is 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 and can add additional hazards using branches off the basic entries. The Cause and Effect Diagram should be used in a team setting whenever possible.

RESOURCES: There are many publications describing in great detail how to use Cause and Effect Diagrams.[28]

EXAMPLES: An example of the Cause and Effect Tool in action follows.

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

[28] K. Ishikawa, Guide to Quality Control, Quality Resources, White Plains, New York, 12th Printing 1994.

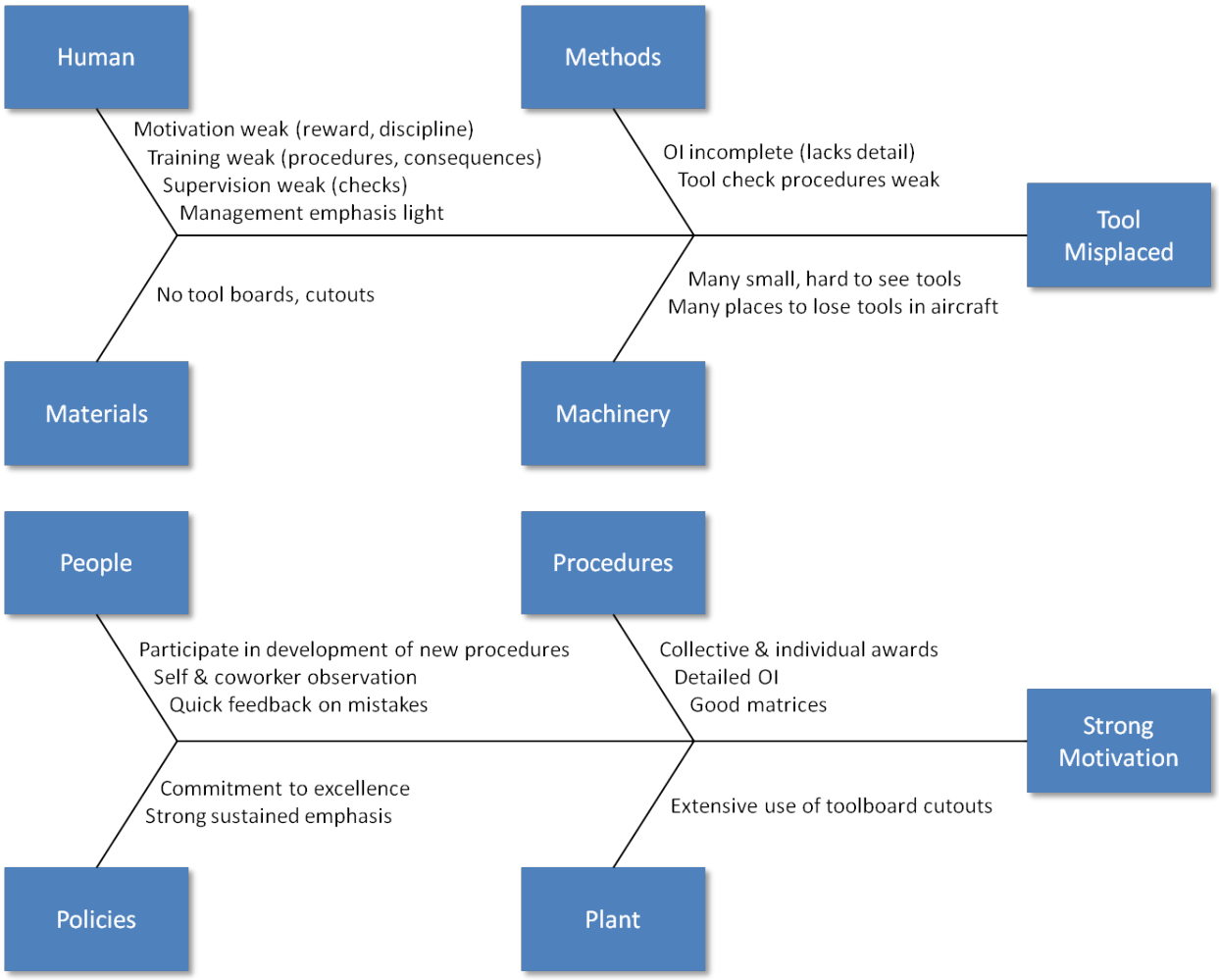


Figure C-4: Cause and Effect Diagram

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

C.2.3. Change Analysis

PURPOSE: Change is a potential source of risk in operational processes. The figure below illustrates this causal relationship.

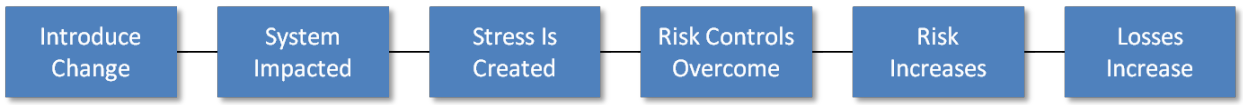


Figure C-5: Change Causation

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, just 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: The 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 important 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 on the next page. The factors in the column on the left side of this tool are intended as a comprehensive change checklist.

RESOURCES: Experienced operational personnel are a key resource for the Change Analysis tool. Those who have long term involvement in an operational process must help define the “comparable situation.” Another important resource is the documentation of process flows and task analyses. Large numbers of such analyses have been completed in recent years in connection with quality improvement and reengineering projects. These materials are excellent definitions of the baseline against which change can be evaluated.

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 a 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, Scenario Process Tool, or other specialized analyses.

C.2.4. Common Cause Failure Analysis (CCFA)

OVERVIEW: The Common Cause Failure Analysis (CCFA) is an extension of the Fault Tree Analysis (FTA) and is used to identify "coupling factors" that can cause component failures to be potentially interdependent. Primary events of minimal cut sets from the FTA are examined through the development of matrices to determine if failures are linked to some common cause relating to environment, location, secondary causes, human error, or quality control. A cut set is a set of basic events (e.g., a set of component failures) whose occurrence causes the system to fail. A minimum cut set is one that has been reduced to eliminate all redundant "fault paths." The CCFA provides a better understanding of the interdependent relationship between FTA events and their causes. It analyzes safety systems for "real" redundancy. This analysis provides additional insight into system failures after the development of a detailed FTA when data on components, physical layout, operators, and inspectors are available.

C.2.5. Comparative Safety Assessment (CSA)

OVERVIEW: The Comparative Safety Assessment (CSA) is an analysis type that provides management with a listing of all the hazards associated with a design change, along with a Comparative Safety Assessment for each alternative hazard combination considered. The CSA for a given proposal or design change expands the Preliminary Hazard List (PHL) developed for the Operational Safety Assessment (OSA). The OSA provides an essential input into CSA safety assessments that support trade studies and decision making in the operational and acquisition processes. The CSA's broad scope is an excellent way to identify issues that may require the use of more detailed hazard identification tools.

Selection of some alternate design elements, e.g., operational parameters and/or architectural components or configuration in lieu of others, implies recognition on the part of management that one set of alternatives will result in either more or less risk of an accident. The risk management concept emphasizes the identification of the change in risk with a change in alternative solutions.

The CSA is also a planning tool. It requires planning for the development of safety operating procedures and test programs to resolve uncertainty when safety risk cannot be completely controlled by design. It provides a control system to track and measure progress towards the resolution of uncertainty and to measure the reduction of safety risk.

The following is a sample CSA Template.[29]

[29] Refer to the Air Traffic Organization's (ATO's) Safety Risk Management Guidance for System Acquisitions (SRMGSA) document for new acquisitions where the Acquisition Management System applies.

CSA Template

Hazard Name	Hazard Description	Causes	System States	Effects	Severity/ Rationale	Existing Safety Solutions	Alternative Solutions					
							Alternative 1	Alternative 1 Risk	Alternative 2	Alternative 2 Risk	Alternative 3	Alternative 3 Risk

C.2.6. Crow-AMSAA Reliability Growth Model

OVERVIEW: Crow-AMSAA is an analytical technique that is used to model event data and forecast the number and timing of future occurrences of those events. Crow-AMSAA is used to plot the cumulative number of events against the cumulative service time. Since only cumulative time is needed, Crow-AMSAA allows for failure modeling even if the time on each unit in the at-risk population is unknown. For this reason, it allows very powerful analyses on relatively limited data. It also works well in situations with serious deficiencies in the data, including missing data and unidentified sub-populations.

The parameters of the Crow-AMSAA model are β, the slope, and λ, the intercept or scale parameter. Changes in failure rate can be detected through obvious slope changes.

METHOD: The Crow-AMSAA model takes advantage of the linear relationship between the logarithm of cumulative failures or other events and the logarithm of cumulative operational or test time. If the analyst plots cumulative failures vs. cumulative time on log-log graph paper, a best-fit straight line can be visually fit through the data. This line has the formula:

$$n(t) = \lambda t^{\beta}$$

where n(t) is cumulative events, t is cumulative time, β is the slope as read off the log-log paper, and λ is the intercept of the line with the Y axis at t=1. The more common methodology is to use a computer software program to perform the analysis and provide the best fit automatically. The software programs will also evaluate the significance of changes in the slope and thus the event rate.

Once the line has been made, it can be extrapolated to predict the future number of events as total time increases. This enables the analyst to model the future reliability of the system over the next month, year, and beyond.

RESOURCES: Various commercially available software programs exist. FAA Aircraft Certification has a site license for SuperSmith™ by Fulton Findings, LLC. This program will perform Crow-AMSAA.

EXAMPLE: The following plot is an example of a Crow-AMSAA analysis analyzing failures in a component. Note the slope change showing an increasing failure rate. In this example, the changed failure rate was due to a new failure mode introduced due to a manufacturing change to fix the prior problem. The timing of the slope change on the plot helped to highlight where to look for underlying causes of the change.

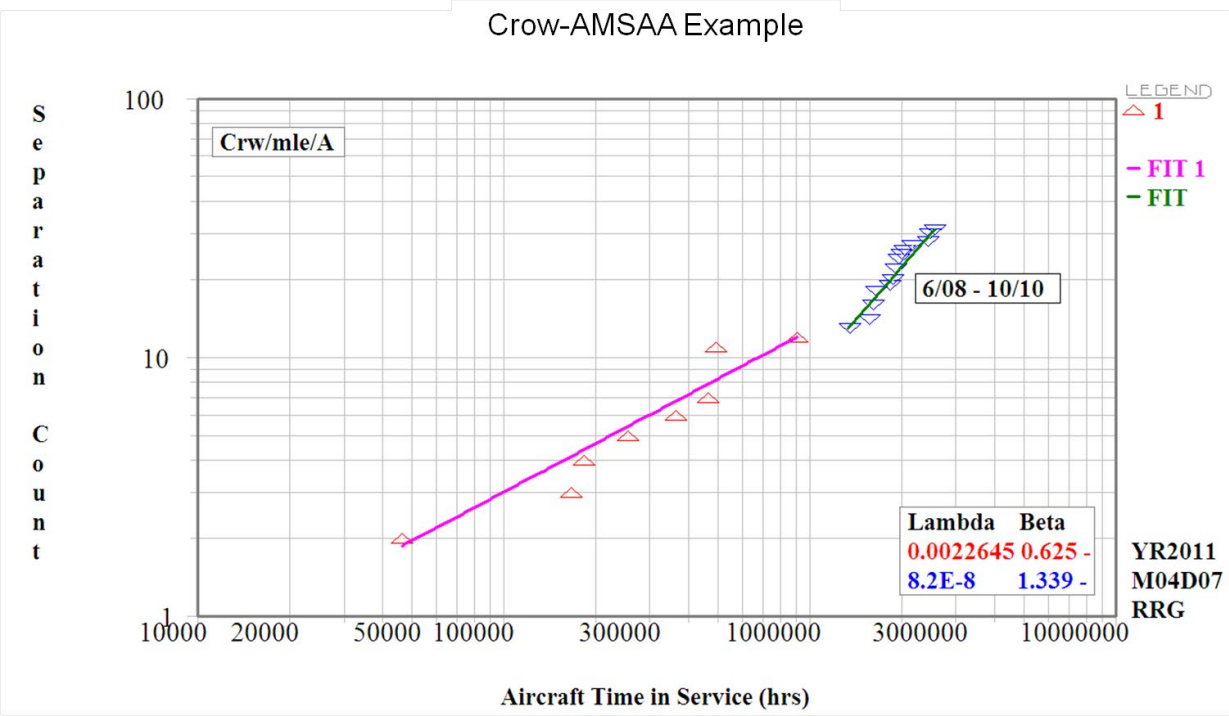


Figure C-6: Crow-AMSAA Example Plot

C.2.7. Energy Trace Analysis (ETA)

OVERVIEW: The Energy Trace Analysis (ETA) is a hazard analysis approach used to address all sources of uncontrolled and controlled energy that have the potential to cause an accident. Examples include utility electrical power and aircraft fuel. Sources of energy causing accidents can be associated with the product or process (e.g., flammability or electrical shock), the resource if different than the product/process (e.g., smoking near flammable fluids), and the items/conditions surrounding the system or resource of concern (e.g., vehicles or taxiing aircraft). A large number of hazardous situations are related to uncontrolled energy associated with the product or the resource being protected (e.g., human error). Some hazards are passive in nature (e.g., sharp edges and corners are a hazard to a maintenance technician working in a confined area).

The purpose of the ETA is to ensure that all hazards and their immediate causes are identified. Once the hazards and their causes are identified, they can be used as top events in a Fault Tree or used to verify the completeness of a Fault Hazard Analysis (FHA). Consequently, the energy trace analysis method complements but does not replace other analyses, such as Fault Tree Analyses, Sneak Circuit Analyses, event trees, and Failure Mode and Effects Analyses (FMEAs).

Identification of energy sources and energy transfer processes is the key element in the energy source analysis procedure. Once sources of energy have been identified, the analyst eliminates or controls the hazard using the Safety Order of Precedence.

These analyses point out potential unwanted conditions that could conceivably happen. Each condition is evaluated further to assess its hazard potential.

METHOD: Understanding the energy trace analysis can be facilitated by examining the analysis steps below.

1. Identify the resource being protected (personnel or equipment) to guide the direction of the analysis toward the identification of only those conditions (i.e., hazards) that would be critical or catastrophic from a mission viewpoint.
2. Identify system and sub-systems, and safety critical components.
3. Identify the operational phase(s), such as preflight, taxi, takeoff, cruise, landing, that each system/sub-system/component will experience. It is often desirable to report results of hazard analyses for each separate operational phase.
4. Identify the operating states for the sub-systems/components (e.g., on/off, pressurized, hot, cooled) during each operational phase.
5. Identify the type(s) of energy present in the identified system.
6. Identify the energy sources or transfer modes that are associated with each sub-system and each operating state. A list of general energy source types and energy transfer mechanisms follows.

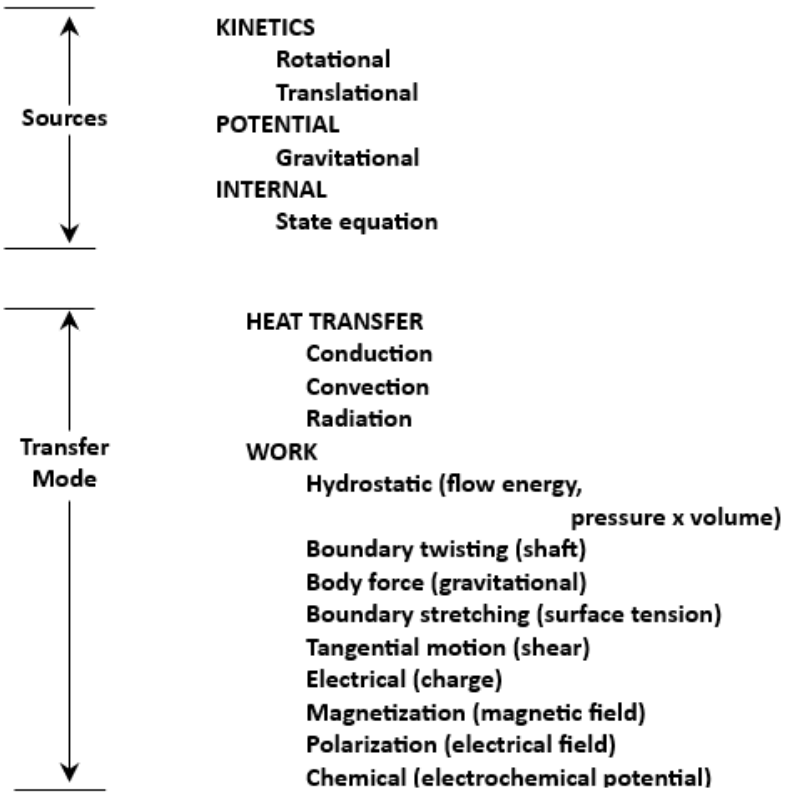


Figure C-7: Energy Sources and Transfer Modes

7. Identify the energy release mechanism for each energy source (released or transferred in an uncontrolled/unplanned manner). It is possible that a normal (i.e., as designed) energy release could interact adversely with other components in a manner not previously or adequately considered.

8. Review a generic threat checklist for each component and energy source or transfer mode. Experience has shown that certain threats are associated with specific energy sources and components.
9. Identify causal factors associated with each energy release mechanism. A hazard causal factor may have subordinate or underlying causal factors associated with it. For instance, excessive stress may be a “top level” factor. The excessive stress may, in turn, be caused by secondary factors such as inadequate design, material flaws, poor quality welds, and excessive loads due to pressure or structural bending. By systematically evaluating such causal factors, an analyst may identify potential design or operating deficiencies that could lead to hazardous conditions. Causal factors are identified independent of the probability of occurrence of the factor; the main question to be answered is: can the causal factor occur or exist?
10. Identify the potential accident that could result from energy released by a particular release mechanism.
11. Define the hazardous consequences that could result given the accident specified in the previous step.
12. Evaluate the hazard category (i.e., critical, catastrophic, or other) associated with the potential accident.
13. Identify the specific hazard associated with the component and the energy source or transfer mode relative to the resource being protected.
14. Recommend actions to control the hazardous conditions.
15. Specify verification procedures to assure that the controls have been implemented adequately.

There are some risk/hazard control methodologies that lend themselves to an energy source hazard analysis approach. These include the following strategies:

- Prevent the accumulation of potential energy by setting limits on noise, temperature, pressure, speed, voltage, loads, quantities of chemicals, amount of light, storage of combustibles, and height of ladders.
- Prevent the release of potential energy through engineering design, containment vessels, gas venting, insulation, safety belts, and lockouts.
- Modify the release of energy by using shock absorbers, safety valves, rupture discs, blowout panels, and less incline on the ramps.
- Separate assets from energy (in either time or space) by moving people away from hot engines, limiting the exposure time, and using thermal or electrically insulated gloves.
- Provide blocking or attenuation barriers, such as eye protection, gloves, respiratory protection, sound absorption, ear protectors, welding shields, fire doors, sunglasses, and machine guards. Raise the damage or injury threshold by improving the design (strength, size), immunizing against disease, or warming up by exercise.
- Establish contingency responses such as early detection of energy release, first aid, emergency showers, general disaster plans, and recovery of system operation procedures.

C.2.8. Energy Trace and Barrier Analysis (ETBA)

ALTERNATIVE NAMES: Abnormal energy exchange

PURPOSE: The Energy Trace and Barrier Analysis (ETBA) is a procedure used 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 loss system safety professionals and is used to analyze 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 involves five basic steps.

ETBA 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 damage something significant).
Step 5. Develop improved controls and implement as appropriate.

Step 1 is the identification of the types of energy found in the system. It often requires considerable expertise to detect the presence of the types of energy listed below.

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)

Step 2 is the trace step. Once identified as present, the point of origin of a particular type of energy must be determined and then the flow of that energy through the system must be traced.

In Step 3 the barriers to the unwanted release of that energy must be analyzed. For example, electrical energy is usually moved in wires with an insulated covering.

In Step 4 the risk of barrier failure and the unwanted release of the energy are assessed.

Finally, in Step 5, risk control options are considered and selected.

RESOURCES: This tool requires a sophisticated understanding of the technical characteristics of systems and of the various energy types and barriers. Availability of a safety professional, especially a safety engineer or other professional engineer is important.

EXAMPLES: A simplified example of the ETBA procedure follows.

Example ETBA

Scenario: The supervisor of a maintenance facility has just investigated a serious incident involving one of his personnel who received a serious shock while using a portable power drill in the maintenance area. The tool involved used a standard three-prong plug. Investigation revealed that the tool and the receptacle were both functioning properly. The individual was shocked when he was holding the tool and made contact with a piece of metal electrical conduit (the one his drill was plugged into) that had become energized as a result of an internal fault. The current flowed through the individual to the tool and through the grounded tool to the ground, resulting in the severe shock. The supervisor decides to fully assess the control of electrical energy in this area.

Option 1. Three prong tool. Electrical energy flow that is from the source through an insulated wire, to the tool, to a single insulated electric motor. In the event of an internal fault, the flow is from the case of the tool through the ground wire to the ground through the grounded third prong through a properly grounded receptacle.

Hazards: Receptacle not properly grounded, third prong removed, person provides lower path of resistance, break in any of the ground paths (case, cord, plug, and receptacle). These hazards are serious in terms of the frequency encountered in the work environment and might be expected to be present in 10% or more cases.

Option 2. Double insulated tool. The tool is not grounded. Protection that is provided by double insulating the complete flow of electrical energy at all points in the tool. In the event of an internal fault, there are two layers of insulation protection between the fault and the person preventing shorting through the user.

Hazards: If the double layers of insulation are damaged as a result of extended use, rough handling, or repair/maintenance activity, the double insulation barrier can be compromised. In the absence of a fully effective tool inspection and replacement program, such damage is not an unusual situation.

Option 3. Grand Fault Circuit Fault Interrupters. Either of the above types of tools are used (double insulated is preferred). Electrical energy flows as described above in both the normal and fault situations. However, in the event of a fault (or any other cause of a differential between the potential of a circuit), it is detected almost instantly, and the circuit is opened, preventing the flow of dangerous amounts of current. Because no dangerous amount of current can flow, the individual using the tool is in no danger of shock. Circuit interrupters are reliable at a level of 1 in 10,000 or higher and when they do fail, most failure modes are in the fail-safe mode. Ground Fault circuit fault interrupters are inexpensive to purchase and relatively easy to install. In this case, the best option is very likely to be the use of the circuit interrupter in connection with either Option 1 or 2, with 2 the preferred. This combination, for all practical purposes, eliminates the possibility of electric shock and injury/death as a result of using portable power tools.

C.2.9. Expected Value Tool

PURPOSE: The Expected Value Tool is an Excel-based tool that automatically converts the FAA 8040.4C likelihood definitions into expected value definitions based on an assigned exposure.

APPLICATION: The Expected Value Tool can only be used with the methodology, definitions, and risk matrices in FAA Order 8040.4C.

METHOD: SRM Teams enter the exposure into the specified cell and use the expected value definitions to determine the likelihood category. The Expected Value Tool can be accessed via the FAA SRM Intranet page.

C.2.10. Failure Mode and Effects Analysis (FMEA)

PURPOSE: The Failure Mode and Effects Analysis (FMEA) is designed to evaluate the impact due to the failure of various system components. A brief example of FMEA illustrating this purpose is the analysis of the impact of the failure of the communications component (radio, landline, computer, etc.) of a system on the overall operation. The focus of the FMEA is on how such a failure could occur (failure mode) and the impact of such a failure (effects).

APPLICATION: The FMEA is generally regarded as a reliability tool, but most operational personnel can use the tool effectively. The FMEA can be thought of as a more detailed "What If" analysis. It is especially useful in contingency planning, where it is used to evaluate the impact of various possible failures (contingencies). The FMEA can be used in place of the "What If" analysis when greater detail is needed, or it can be used to examine the impact of hazards developed using the "What If" tool in much greater detail.

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. A frozen bearing (component) or a shaft unable to turn (function) are valid failure modes.

METHOD: The approach to generating an FMEA is comparable to that of the Fault Hazard Analysis (FHA). The first step is to list all components or low-level functions. Then, by examining system block diagrams, schematics, etc., the function of each component is identified. Next, all reasonably possible failure modes of the lowest "component" being analyzed are identified. Using a coolant pump bearing as an example, they might include a frozen bearing, high friction, or too much play. For each identified failure mode, the effect at the local level, an intermediate level, and the top system level are recorded. A local effect might be "the shaft won't turn," an intermediate effect might be "pump won't circulate coolant," and a system-level effect might be "engine overheat and fail." At this point in the analysis, the FMEA might identify a hazard.

The analyst next documents the method of fault detection. This input is valuable for designing self-test features or the test interface of a system. More importantly, it can alert an air crew to a failure in process prior to a catastrophic event. A frozen pump bearing might be detected by monitoring power to the pump motor or coolant temperature. Given adequate warning, the engine can be shut down before damage takes place or the aircraft can land prior to engine failure. Next, compensating provisions are identified as the first step in determining the impact of the failure. If there are redundant pumps or combined cooling techniques, the significance of the failure is less than if the engine depends on a single pump. The severity categories used for the

hazard analysis can be used as the severity class in the FMEA. A comments column is usually added to the FMEA to provide additional information that might assist the reviewer in understanding any FMEA column.

The FMEA uses a worksheet similar to the one that follows. As noted on the sample worksheet, a specific component of the system to be analyzed is identified. Several components can be analyzed. For example, a rotating part might freeze up, explode, break up, slow down, or even reverse direction. Each of these failure modes may have differing impacts on connected components and the overall system. The worksheet calls for an assessment of the probability of each identified failure mode.

Sample Failure Mode and Effects Analysis Worksheet

FAILURE MODE AND EFFECTS ANALYSIS

Page ___of ___Pages

System_____ Date_____

Sub-system _____ Analyst_____

Component Description	Failure Mode	Effects on Other Components	Effects On System	Hazard Category	Failure Frequency Effects Probability	Remarks

EXAMPLES: An example FMEA showing flight vehicle systems components follows.

Example FMEA

Component Description	Failure Mode	Effects on Other Components	Effects on System	Hazard Category	Failure Frequency Effects Probability	Remarks
Pump bearing	Frozen	Pump failure	Engine failure	Technical – Flight Vehicle Systems	Extremely Improbable	
Pump bearing	High Friction	Loss of cooling capacity	Engine runs hot	Technical – Flight Vehicle Systems	Remote	
Pump bearing	Loose (Wear)	Loss of cooling capacity	Low Horse Power	Technical – Flight Vehicle Systems	Frequent	

C.2.11. Failure Modes, Effects, and Criticality Analysis (FMECA)

OVERVIEW: FMECAs and Failure Mode and Effects Analyses (FMEAs) are important reliability program tools that provide data usable by the SRM Team. 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. An FMECA is generated from an 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 Analysis). 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 analyses: "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.

APPROACH: Adding a criticality figure of merit is needed to generate the FMECA from the FMEA. Assigning severity levels cannot be performed without first identifying the purpose of the FMECA. For example, a component with a high failure rate would have a high severity factor for a reliability analysis; a long lead time or expensive part would be more important in a supportability analysis. Neither may be significant from a safety perspective. Therefore, a safety analysis requires a unique criticality index or equation. The assignment of a criticality index is called a criticality analysis. The Index is a mathematical combination of severity and probability of occurrence (likelihood of occurrence).

Sample Failure Modes, Effects, and Criticality Analysis

Item/ Function	Function	Failure Modes	Failure Local	Next Higher	Effects End Effects	Failure Detection Method	Compensate Provisions	Severity Class
Pump bearing	Facilitate shaft rotation	Frozen	Shaft won't rotate	Pump failure	Engine failure	Engine Temp	Air cooling	I
		High Friction	Shaft turns slowly	Loss of cooling capacity	Engine runs hot	" "	" "	II
		Loose (Wear)	Shaft slips	" "	Low Horse Power	" "	" "	III

Severity Class: I-Catastrophic to IV-Incidental
Not shown are columns that may be added including frequency class, interfaces, and comments.

The FMECA and the hazard analyses provide some redundant information, but more importantly, some complementary information. The hazard analyses consider human factors and systems interface problems; the FMECA does not. The FMECA, however, is not more likely to identify hazards caused by component or software module failure than hazard analyses, which consider compensating and fault detection features.

C.2.12. Fault Hazard Analysis (FHA)

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

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

An FHA can be used for a number of purposes:

- Aid in system design concept selection;
- Support “functional mechanizing” of hardware;
- “Design out” critical safety failure modes;
- Assist in operational planning; and
- Provide inputs to management risk control efforts.

The FHA must consider both “catastrophic” and “out-of-tolerance modes” of failure. For example, a five percent, 5K (plus or minus 250 ohm) resistor can have functional failure modes of failing open or failing short, while the out-of-tolerance modes might include too low or too high a resistance.

To conduct an FHA, it is necessary to know and understand certain system characteristics:

- Equipment mission
- Operational constraints
- Success and failure boundaries
- Realistic failure modes and a measure of their probability of occurrence

METHOD: The procedural steps are:

1. The system is divided into modules (usually functional or partitioning) that can be handled effectively.
2. Functional diagrams, schematics, and drawings for the system and each sub-system are then reviewed to determine their interrelationships and the interrelationships of the component subassemblies. This review may be done by the preparation and use of block diagrams.
3. For analyses performed down to the component level, a complete component list with the specific function of each component is prepared for each module as it is to be analyzed. For those cases when the analyses are to be performed at the functional or partitioning level, this list is for the lowest analysis level.

4. Operational and environmental stresses affecting the system are reviewed for adverse effects on the system or its components.
5. Significant failure mechanisms that could occur and affect components are determined from analysis of the engineering drawings and functional diagrams. Effects of sub-system failures are then considered.
6. The failure modes of individual components that would lead to the various possible failure mechanisms of the sub-system are then identified. Basically, it is the failure of the component that produces the failure of the entire system. However, since some components may have more than one failure mode, each mode must be analyzed for its effect on the assembly and then on the sub-system. This may be accomplished by tabulating all failure modes and listing the effects of each (e.g., a resistor that might fail open or short, high, or low). An understanding of physics of failure is necessary. For example, most resistors cannot fail in a shorted mode. If the analyst does not understand this, considerable effort may be wasted on attempting to control a nonrealistic hazard.
7. All conditions that affect a component or assembly should be listed to indicate whether there are special periods of operation, stress, personnel action, or combinations of events that would increase the probabilities of failure or damage.
8. The risk category should be assigned.
9. Preventative or corrective measures to eliminate or control the risks are listed.
10. Initial probability rates are entered. These are “best judgments” and are revised as the design process goes on. Care must be taken to make sure that the probability represents that of the particular failure mode being evaluated. A single failure rate is often provided to cover all of a component’s failure modes rather than separate ones for each.
11. A preliminary criticality analysis may be performed as a final step.

The FHA has some serious limitations. They include:

- A sub-system is likely to have failures that do not result in accidents. Tracking all of these in the SMS is a costly, inefficient process. If this is the approach to be used, combining it with an FMEA (or FMECA) performed by the reliability program can save some costs.
- This approach concentrates usually on hardware failures, to a lesser extent on software failures, and often inadequate attention is given to human factors. For example, a switch with an extremely low failure rate may be dropped from consideration, but the wrong placement of the switch may lead to an accident. The adjacent placement of a power switch and a light switch, especially of similar designs, will lead to operator errors.
- Environmental conditions are usually considered, but the probability of occurrence of these conditions is rarely considered. This may result in applying controls for unrealistic events.
- Probability of failure leading to hardware related hazards ignores latent defects introduced through substandard manufacturing processes. Thus, some hazards may be missed.
- One of the greatest pitfalls in the FHA (and in other techniques) is over-precision in mathematical analysis. Too often, analysts try to obtain “exact” numbers from “inexact” data, and too much time may be spent on improving preciseness of the analysis rather than on eliminating the hazards.

C.2.13. Fault Tree Analysis (FTA)

OVERVIEW: The Fault Tree Analysis (FTA) is a popular and productive hazard identification tool. It provides a standardized discipline to evaluate and control hazards. The FTA process is used to solve a wide variety of problems ranging from safety to management issues.

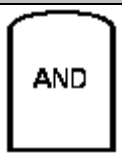
This tool is used by the professional safety and reliability community to both prevent and resolve hazards and failures. Both qualitative and quantitative methods are used to identify areas in a system that are most critical to safe operation. Either approach is effective. The output is a graphical presentation providing technical and administrative personnel with a map of “failure or hazard” paths. The reviewer and the analyst must develop an insight into system behavior, particularly those aspects that might lead to the hazard under investigation.

Qualitative FTAs are cost effective and invaluable safety engineering tools. The generation of a qualitative fault tree is always the first step. Quantitative approaches multiply the usefulness of the FTA but are more expensive and often very difficult to perform.

An FTA (similar to a Logic Diagram) is a deductive analytical tool used to study a specific undesired event such as engine failure. The deductive approach begins with a defined undesired event, usually a postulated accident condition, and systematically considers all known events, faults, and occurrences that could cause or contribute to the occurrence of the undesired event. Top level events may be identified through any safety analysis approach, through operational experience, or through a “Could it happen?” hypothesis.

The FTA is a graphical logic representation of fault events that may occur to a functional system. This logical analysis must be a functional representation of the system and must include all combinations of system fault events that can cause or contribute to the undesired event. Each contributing fault event should be further analyzed to determine the logical relationships of underlying fault events that may cause them. This tree of fault events is expanded until all input fault events are defined in terms of basic, identifiable faults that may then be quantified for computation of probabilities, if desired. When the tree has been completed, it becomes a logic gate network of fault paths, both singular and multiple, containing combinations of events and conditions that include primary, secondary, and upstream inputs that may influence or command the hazardous mode.

EXAMPLE: The following standardized symbology is used.

SYMBOL	DESCRIPTION
	**And gate** - represents a condition in which all the events shown below the gate (input gate) must be present for the event shown above the gate (output event) to occur. This means the output event will occur only if all of the input events exist simultaneously.
	**Or gate** - represents a situation in which any of the events shown below the gate (input gate) will lead to the event shown above the gate (output event). The event will occur if only one or any combination of the input events exists.
	**Rectangle** - The rectangle is the main building block for the analytical tree. It represents the negative event and is located at the top of the tree and can be located throughout the tree to indicate other events capable of being broken down further. This is the only symbol that will have a logic gate and input events below it.
	**Circle** – A circle represents a base event in the tree. These are found on the bottom tiers of the tree and require no further development or breakdown. There are no gates or events below the base event.
	**Diamond** – The diamond identifies an undeveloped terminal event. Such an event is one not fully developed because of a lack of information or significance. A fault tree branch can end with a diamond. For example, most projects require personnel, procedures, and hardware. The tree developer may decide to concentrate on the personnel aspect of the procedure and not the hardware or procedural aspects. In this case the developer would use diamonds to show “procedures” and “hardware” as undeveloped terminal events.
	**Oval** – An oval symbol represents a special situation that can only happen if certain circumstances occur. This is spelled out in the oval symbol. An example of this might be if switches must be thrown in a specific sequence before an action takes place.
	**Triangle** – The triangle signifies a transfer of a fault tree branch to another location within the tree. Where a triangle connects to the tree with an arrow, everything shown below the connection point transfers to another area of the tree. This area is identified by a corresponding triangle that is connected to the tree with a vertical line. Letters, numbers or figures identify one set of transfer symbols from another. To maintain the simplicity of the analytical tree, the transfer symbol should be used sparingly.

A non-technical person can, with minimal training, determine from the fault tree, the combination and alternatives of events that may lead to failure or a hazard. The following is a sample FTA for an aircraft engine failure. In this sample, there are three possible causes of engine failure: fuel flow, coolant, or ignition failure. The alternatives and combinations leading to any of these conditions may also be determined by inspection of the FTA.

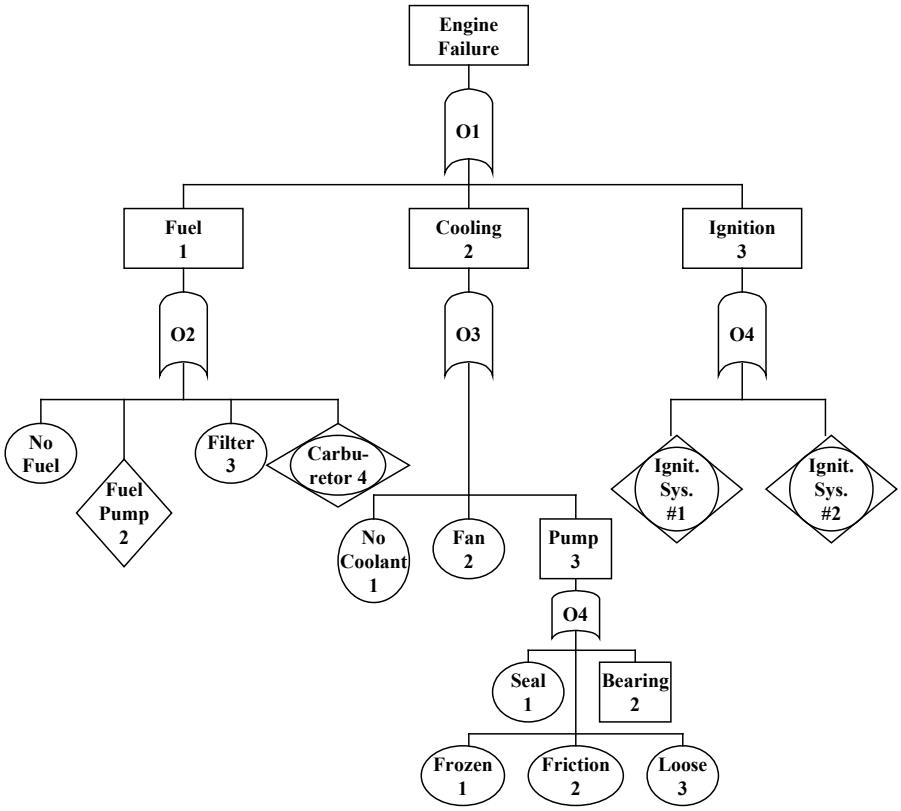


Figure C-8: Sample Engine Failure Fault Tree

Based on available data, probabilities of occurrences for each event can be assigned. Algebraic expressions can be formulated to determine the probability of the top-level event occurring. This can be compared to acceptable thresholds and the necessity and direction of corrective action determined.

The FTA shows the logical connections between failure events and the top-level hazard or event. “Event,” the terminology used, is an occurrence of any kind. Hazards and normal or abnormal system operations are examples. For example, both “engine overheats” and “frozen bearing” are abnormal events. Events are shown as some combination of rectangles, circles, triangles, diamonds, and “houses.” Rectangles represent events that are a combination of lower-level events. Circles represent events that require no further expansion. Triangles reflect events that are dependent on lower-level events where the analyst has chosen to develop the fault tree further. Diamonds represent events that are not developed further, usually due to insufficient information. Depending upon criticality, it may be necessary to develop these branches further.

Another event symbol not pictured is called a “house.” That symbol illustrates a normal (versus failure) event. If the hazard were “unintentional stowing of the landing gear,” a normal condition for the hazard would be the presence of electrical power. FTA symbols can depict all aspects of the NAS events. The example reflects a hardware-based problem. More typically, software

(e.g., incorrect assumptions or boundary conditions), human factors (e.g., inadequate displays), and environment conditions (e.g., ice) are also included, as appropriate.

Events can be further broken down as primary and secondary. A primary event is a coolant pump failure caused by a bad bearing. A secondary event would be a pump failure caused by ice through the omission of antifreeze in the coolant on a cold day. The analyst may also distinguish between faults and failures. An ignition turned off at the wrong time is a fault; an ignition switch that will not conduct current is an example of failure.

Events are linked together by “AND” and “OR” logic gates. The latter is used in the example for both fuel flow and carburetor failures. For example, fuel flow failures can be caused by either a failed fuel pump or a blocked fuel filter. An “AND” gate is used for the ignition failure, illustrating that the ignition systems are redundant. That is, both must fail for the engine to fail. These logic gates are called Boolean gates or operators. Boolean algebra is used for the quantitative approach. The “AND” and “OR” gates are numbered sequentially A# or O# respectively in the diagram.

As previously stated, the FTA is built through a deductive “top down” process. It is a deductive process in that it considers combinations of events in the “cause” path as opposed to the inductive approach, which does not. The process is asking a series of logical questions such as “What could cause the engine to fail?” When all causes are identified, the series of questions is repeated at the next lower level, i.e., “What would prevent fuel flow?” Interdependent relationships are established in the same manner.

When a quantitative analysis is performed, probabilities of occurrences are assigned to each event. The values are determined through analytical processes such as reliability predictions, engineering estimates, or the reduction of field data (when available). A completed tree is called a Boolean model. The probability of occurrence of the top-level hazard is calculated by generating a Boolean equation. It expresses the chain of events required for the hazard to occur. Such an equation may reflect several alternative paths. Boolean equations rapidly become very complex for simple looking trees. They usually require computer modeling for solution. In addition to evaluating the significance of a risk and the likelihood of occurrence, FTAs facilitate presentations of the hazards, causes, and discussions of safety issues.

The FTA's graphical format is superior to the tabular or matrix format in that the inter-relationships are obvious. The FTA graphic format is a good tool for the analyst not knowledgeable of the system being examined. The matrix format is still necessary for a hazard analysis to pick up severity, criticality, family tree, and other information. Being a top-down approach, in contrast to the Fault Hazard Analysis (FHA) and Failure Modes, Effects, and Criticality Analysis (FMECA), the FTA may miss some non-obvious top-level hazards.

C.2.14. Hazard Analysis Worksheet (HAW)

OVERVIEW: The HAW is a worksheet used to document a safety analysis. Using the HAW helps SRM Teams overcome the tendency to focus on safety risk in one aspect of an operation and overlook more serious issues elsewhere in the operation. Its broad scope guides the identification of issues that may require analysis with more detailed hazard identification tools.

It is an initial effort to document the risk assessment of the selected system or change. The Preliminary Hazard Assessment (PHA) and HAW are the most common tools used in safety analyses. In either form, it is a document used to follow the identified hazards through the entire SRM analysis phase. The key idea of the PHA/HAW is to consider the hazards inherent to all aspects of an operation without regard to risk. Safety professionals use the PHA/HAW in nearly all risk management applications except in the most time-critical situations. Depending on the type and complexity of the issue/change, analysis beyond completing a PHA/HAW may not be necessary.

Entries in the PHA/HAW columns represent the minimum information necessary for hazard analysis:

- Hazard ID
- Hazard Description
- Causes
- System State
- Existing Controls
- Existing Control Justification/Supporting Data
- Effects
- Severity
- Severity Rationale
- Likelihood
- Likelihood Rationale
- Initial Risk
- Safety Requirements
- Organization Responsible for Implementing Safety Requirements
- Predicted Residual Risk
- Safety Performance Measures

The following sample HAW is available for download on the SRM Guidance website.

Hazard ID	Hazard Description	Cause	System State	Controls	Control Justification	Effect	Severity	Severity Rationale	Likelihood	Likelihood Rationale	Initial Risk
Use alpha-numeric identifier	Describe the real or potential condition for which the safety analysis is being performed	- Describe the origin of the hazard - (Note: multiple causes can exist for each hazard)	- Describe the various conditions in which a system can exist - (Note: multiple system states can exist for each hazard)	1. Identify mitigation(s) that are currently in place that prevent(s) or reduce(s) the likelihood of the hazard or mitigates its effects	1. Provide a rationale for each control identified in the previous column 2. Provide specific data to support each control, when available 3. Provide any limitations or applicable system state(s) for each control (e.g., whether the control only applies to commercial operations)	Identify possible outcomes that have occurred or have the possibility of occurring Describe an effect for each hazard and given system state	Identify all numerical classifications describing the consequences of the outcomes of the hazard (Scale of 1 through 5, 1 - Catastrophic, 5 - Minimal)	Explain how the severity rating was determined	Identify the estimated frequency of each outcome of the hazard (Scale of A through G; A - Frequent, G - Extremely Improbable)	Explain how the likelihood rating was determined. Provide calculations used to determine probability.	**Identify the combination of the severity and likelihood ratings for the hazard (For Example 3C); color code the column (R/Y/G) accordingly**

Hazard ID	Hazard Description	Safety Recommendations	Mitigation Owner	Timeframe*	Current Risk	Predicted Residual Risk	Predicted Residual Risk Rationale
Use alpha-numeric identifier	Describe the real or potential condition for which the safety analysis is being performed	1. Include safety recommendations	1. Include organization designations	1. Estimate the timeframe by which the recommendation could be completed (short term = 6 months, mid-term = 2 years, long term = more than 2 years)	Identify the combination of the severity and likelihood ratings for the hazard (For Example 3C); color code the column (R/Y/G) accordingly	Identify the combination of the severity and likelihood ratings for the hazard (For Example 3C); color code the column (R/Y/G) accordingly	Explain how the predicted residual risk was determined

* The timeframes are defined as follows: short term is estimated completion within 6 months, mid-term is estimated completion within two years, and long term is estimated completion in more than two years.

Monitoring Plan

Hazard ID	Hazard Description	Initial Risk	Predicted Residual Risk	Monitoring Activities	Data Owner(s)	Reporting Frequency	Reporting Duration	Safety Performance Targets
Use alpha-numeric identifier	Describe the real or potential condition for which the safety analysis is being performed	Identify the combination of the severity and likelihood ratings for the hazard (For Example 3C); color code the column (R/Y/G) accordingly	Identify the combination of the severity and likelihood ratings for the hazard (For Example 3C); color code the column (R/Y/G) accordingly	Provide a description of how the risk associated with each of the hazards identified in the HAW will be monitored	Provide the organization/ point of contact that will collect the data that will be utilized to carry out the monitoring activities	Define how often the monitoring activities listed in the previous column will be tracked	Define the length of time that the monitoring activities listed in the previous column will be tracked. The duration will begin when all mitigations are implemented.	Identify measurable goals that will be used to verify the implementation of the safety recommendations and validate the predicted residual risk score

C.2.15. Hazard Enterprise Assessment Tool (HEAT)

PURPOSE: HEAT is a decision-support tool that provides a structured, data-driven methodology for SRM assessments. It identifies areas in safety risk assessments that require SME knowledge and utilizes their qualitative input in conjunction with quantitative safety data drawn from the NTSB aviation accident database and AIDS.

METHOD: HEAT's risk calculations are driven by a Model-Based Systems Engineering (MBSE) risk framework, which is fully compliant with FAA Order 8040.4C. This risk framework, along with the standardized hazard taxonomy, can make the process of identifying hazards and conducting complex risk calculations more accurate, repeatable, and consistent. The tool can be accessed on the FAA Intranet via this link: HEAT.

C.2.16. The Hazard and Operability Tool (HAZOP)

ALTERNATIVE NAMES: The HAZOP analysis

PURPOSE: The special role of the HAZOP is hazard analysis of completely new operations. In these situations, traditional intuitive and experiential hazard identification procedures are especially weak. This lack of experience weakens 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 going to be undertaken. The issue should be one where there seems to be significant risk because the HAZOP does demand 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 dig very deeply into the operation to identify what that "something" is.

METHOD: The HAZOP is the most highly structured of the hazard identification procedures. It uses a standard set of guide terms which are then linked in every possible way with a tailored set of process terms. 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 in 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.

C.2.17. Interface Analysis

ALTERNATIVE NAMES: Interface Hazard Analysis

PURPOSE: The Interface Analysis is intended to uncover the hazardous linkages or interfaces between 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 looking at these potential energy transfers between two different activities, we can often detect hazards that are difficult to detect in any other way.

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 clue 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 depicted 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.

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/material 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

RESOURCES: Interface Analyses are best accomplished when personnel from all the involved activities participate, so that hazards and interfaces in both directions can be effectively and knowledgeably addressed.

EXAMPLES: An Interface Analysis using the general outline is shown below.

Example Interface Analysis

SITUATION: Construction of a heavy equipment maintenance facility is planned for the periphery of the complex at a major facility. This is a major complex costing over $2,000,000 and requiring about eight months to complete. The objective is to detect interface issues in both directions. Notice that the analysis reveals a variety of interface issues that need to be thought through carefully.
Energy Interface: Movement of heavy construction equipment Movement of heavy building supplies Movement of heavy equipment for repair Possible hazmat storage/use at the facility ***Personnel Interface:*** Movement of construction personnel (vehicle or pedestrian) through base area Movement of repair facility personnel through base area Possible movement of base personnel (vehicular or pedestrian) near or through the facility ***Equipment Interface:*** Movement of equipment as indicated above ***Supply Interface:*** Possible movement of hazmat through base area Possible movement of fuels and gases Supply flow for maintenance area through base area ***Product Interface:*** Movement of equipment for repair by tow truck or heavy equipment transport through the base area ***Information Interface:*** Damage to buried or overhead wires during construction or movement of equipment Possible Electro-magnetic interference due to maintenance testing, arcing, etc. ***Biomaterial Interface:*** None

C.2.18. Interview Tool

PURPOSE: 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. The purpose of the Interview Tool is to capture the experience of these personnel in ways that are efficient and positive for them. 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. There are many options available to collect interview data. The 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. There are situations in which absolute confidentiality must be assured by not using names in connection with data.

Interview Tool Alternatives

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

RESOURCES: It is possible to operate the interview process facility-wide with the data being supplied to individual units. Hazard interviews can also be integrated into other interview activities. For example, counseling sessions could include a hazard interview segment. In these ways, the expertise and resource demands of the Interview Tool can be minimized.

COMMENTS: The key source of risk is human error. Of all the hazard identification tools, the Interview Tool is potentially the most effective at capturing human error data.

EXAMPLES: The example that follows illustrates several variations of the Interview Tool.

Example Exit Interview Format

Name (optional)_____ Organization _____

1. Describe below incidents, near misses or close calls that you have experienced or seen since you have been in this organization. State the location and nature (i.e., what happened and why) of the incident. If you can't think of an incident, then describe two hazards you have observed.

INCIDENT 1, Location.
What happened and why?

INCIDENT 2, Location
What happened and why?

2. What do you think other personnel can do to eliminate these problems:

Personnel:

Incident 1

Incident 2

Supervisors:

Incident 1

Incident 2

Top Leadership:

Incident 1

Incident 2

C.2.19. Job Hazard Analysis (JHA)

ALTERNATIVE NAMES: The task analysis, job safety analysis, activity hazard analysis, JHA, JSA, AHA

PURPOSE: The purpose of the Job Hazard Analysis (JHA) is to examine in detail the safety considerations of a single job. A variation of the JHA called a task analysis focuses on a single task, i.e., some smaller segment of a "job."

APPLICATION: 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 different tasks should be handled by analyzing each major task separately. The illustration considers risk both to the workers involved, and to the system, as well as risk controls for both. Tools such as the Scenario Process Tool and "What If" 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 can be trained in the JHA process and directed to analyze the jobs they supervise.

Sample Job Hazard Analysis Format

Job Safety Analysis	Job Title or Operation	
Organization Symbol	Job Series	Supervisor
Location/Building Number	Shop Title	Reviewed By
Required and/or Recommended Personal Protective Equipment		Approved By
SEQUENCE OF BASIC JOB STEPS	POTENTIAL HAZARDS	RECOMMENDED ACTION OR PROCEDURE

C.2.20. Job Task Analysis (JTA)

OVERVIEW: The foundation of the performance of a Human Error Analysis (HEA) is a JTA, which describes each human task and sub-task within a system in terms of the perceptual (information intake), cognitive (information processing and decision making), and manual (motor) behaviors required of an operator, maintainer, or support person. The JTA should also identify: the skills and information required to complete tasks, equipment requirements, the task setting, time and accuracy requirements, and the probable human errors and consequences relating to these areas. There are several tools and techniques for performing task analyses, depending on the level of analysis needed.

The JTA is the method or procedure used to reduce a unit of work to its base components. The JTA document consists of a detailed, sequential listing of tasks, subtasks, and elements (if required) with the knowledge and skills that clearly define and completely describe the job.

EXAMPLE: The following is an example of a Sample Pilot job task listing from Advisory Circular (AC) No: 120-54A, Advanced Qualification Program.

SAMPLE PILOT JOB TASK LISTING

1. Ground Operations
2.0 Takeoff
    2.1 Perform Normal Takeoff
        2.1.1 Assess Performance and Environmental Factors
        2.1.2 Perform Takeoff Roll
        2.1.3 Perform Rotation and Liftoff
            2.1.3.1 Rotate aircraft at VR to target pitch angle [PF]
            2.1.3.2 Observe barometric/ADC altimeter increase [PF]
            2.1.3.3 Call out positive rate [PM]
            2.1.3.4 Retract Gear [PF, PM]
            2.1.3.5 Establish Climb Speed [PF]
    2.2 Perform Instrument Takeoff
    2.3 Perform Engine Failure after V_1 Takeoff
    2.4 Perform Rejected Takeoff
3. Climb Operations
4. Cruise Operations
5. Descent Operations
6. Approach Operations
    6.1 Perform Approach
        6.1.1 Perform Visual Approach
        6.1.2 Perform Non-Precision Approach Procedures (VOR, NDB, LOC, LOC/BC, LDA, SDF, ASR, RNav/FMS, GPS)
        6.1.3 Perform Cat II ILS
        6.1.4 Perform Cat IIIb ILS
        6.1.5 Perform Coupled Autopilot Approach and Autoland Procedures
    6.2 Perform One Engine Inoperative Cat I ILS Approach and Landing
    6.3 Perform One Engine Inoperative Missed Approach
    6.4 Perform Visual Approach and Rejected Landing
7. Landing Operations
    7.1 Normal Configuration
    7.2 Autoland
    7.3 No-Flap
8. After Landing Operations
9. Aircraft Systems Operations
10. Abnormal and Emergency Procedures
11. Supplementary Procedures

RESOURCES: See pages 14-16 of AC No: 120-54A, Advanced Qualification Program for more information and samples of the JTA.

C.2.21. Logic Diagram

ALTERNATIVE NAMES: The Logic Tree

PURPOSE: The Logic Diagram is intended to provide considerable 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 the 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, an important purpose of the Logic Diagram is to establish 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. By its nature, it is also most effective with more complicated operations in which several hazards may be interlinked in various ways. Because it is more complicated than the other primary tools, it requires more practice, and may not appeal to all operational personnel.

METHOD: There are three types of Logic Diagrams. They 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 factors that must be in place to 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 the various Logic Diagram options can be applied either to an actual operating system or one being planned. Of course, the best time for application is in the planning stages of the operational life cycle. All 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 a positive diagram or negative diagram, the user 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 lots of changes and variations marked on it. With the addition of a whiteboard, it becomes an excellent group tool.

Below is a generic diagram. It is followed by a simplified example of each of the types of Logic Diagrams.

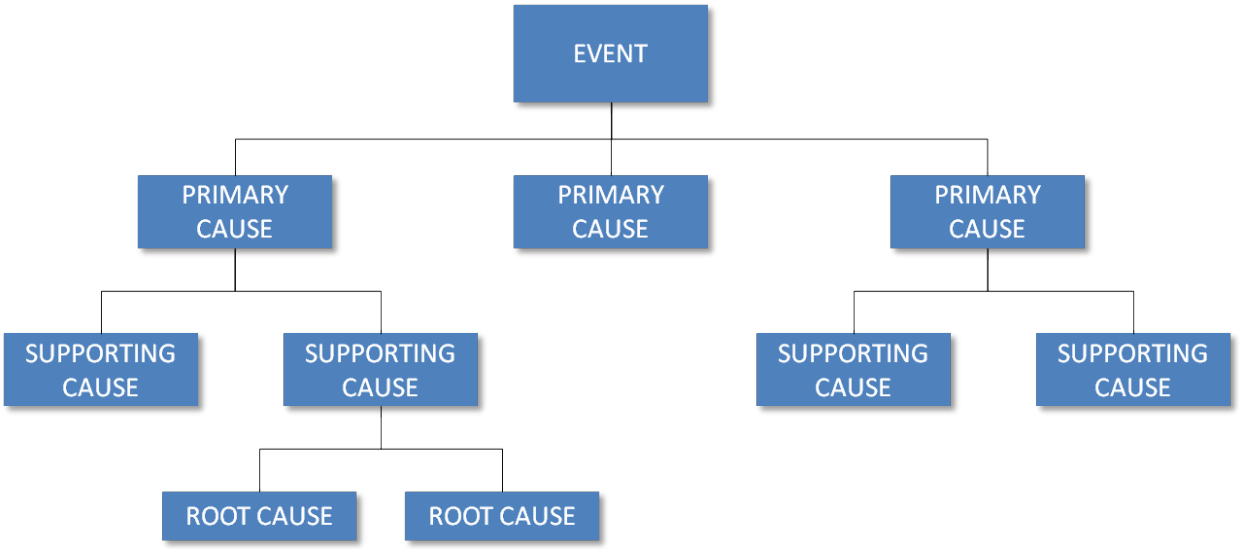


Figure C-9: Generic Logic Diagram

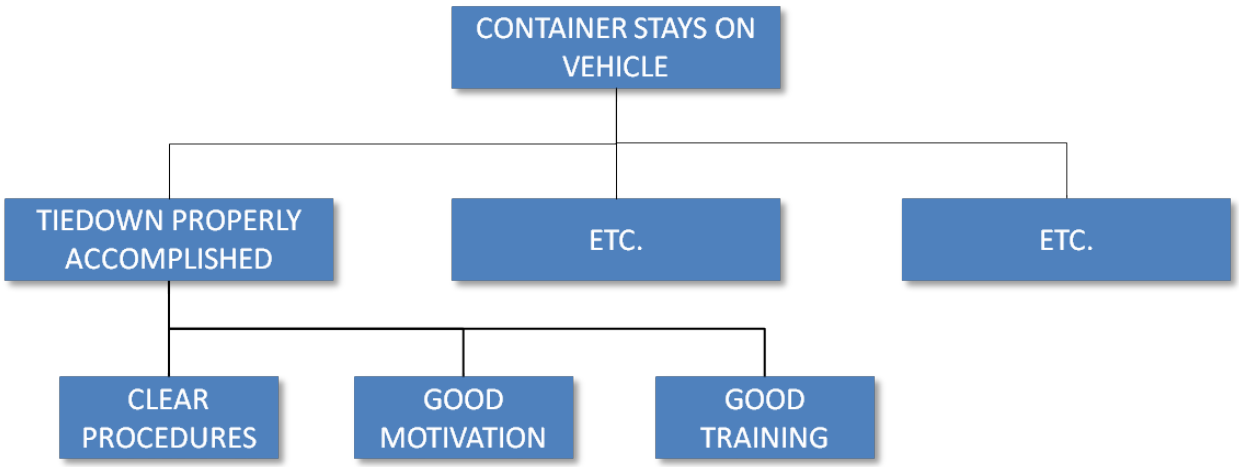


Figure C-10: Positive Event Logic Diagram

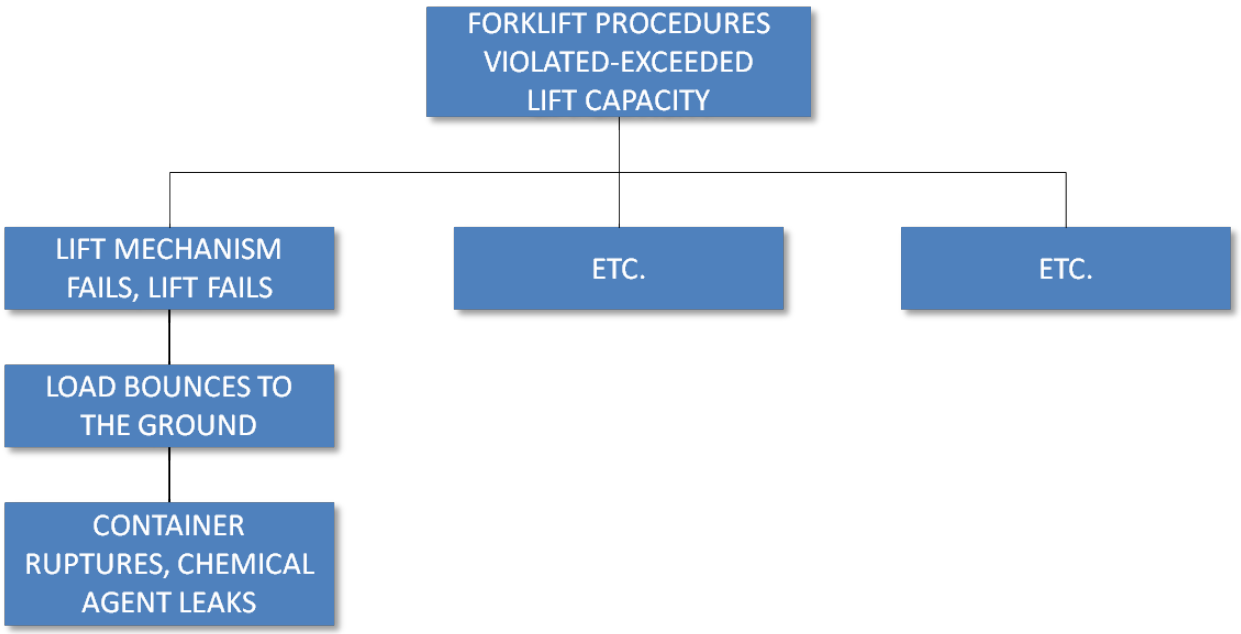


Figure C-11: Risk Event Diagram

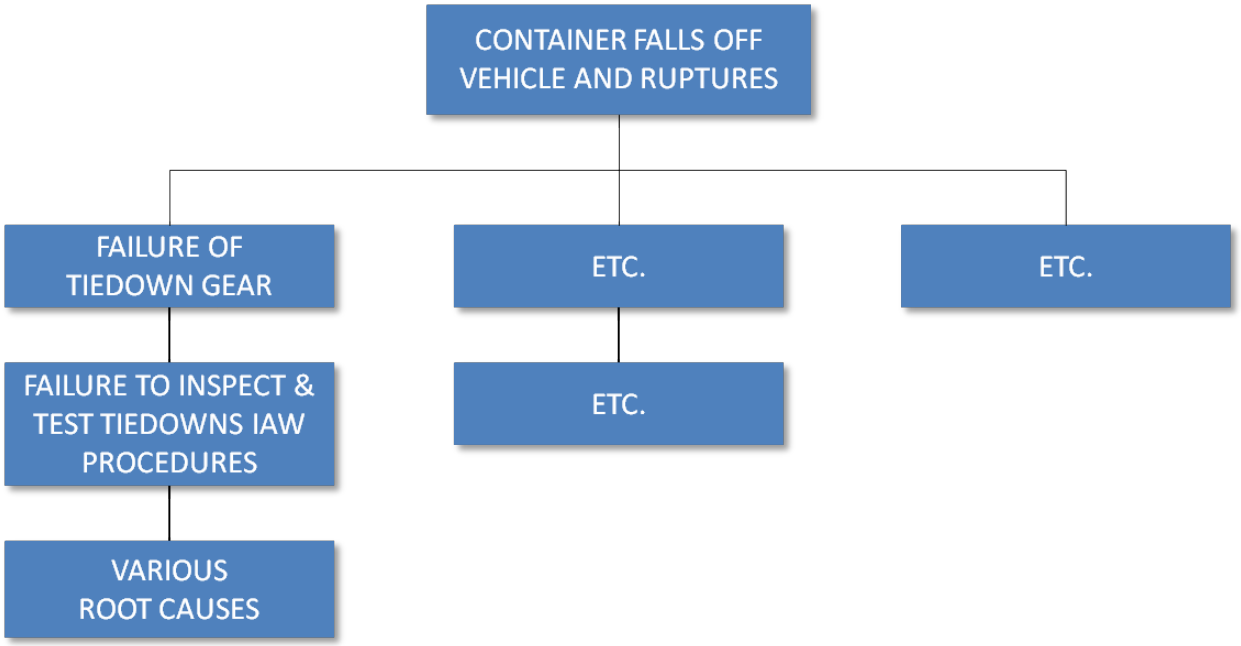


Figure C-12: Negative Event Logic Diagram

RESOURCES: All the other primary tools are key resources for the Logic Diagram, as it can correlate hazards that they generate. If available, a safety professional may be an effective facilitator for the Logic Diagram process.

EXAMPLE: The following illustration shows how a negative diagram could be constructed for moving a heavy piece of equipment.

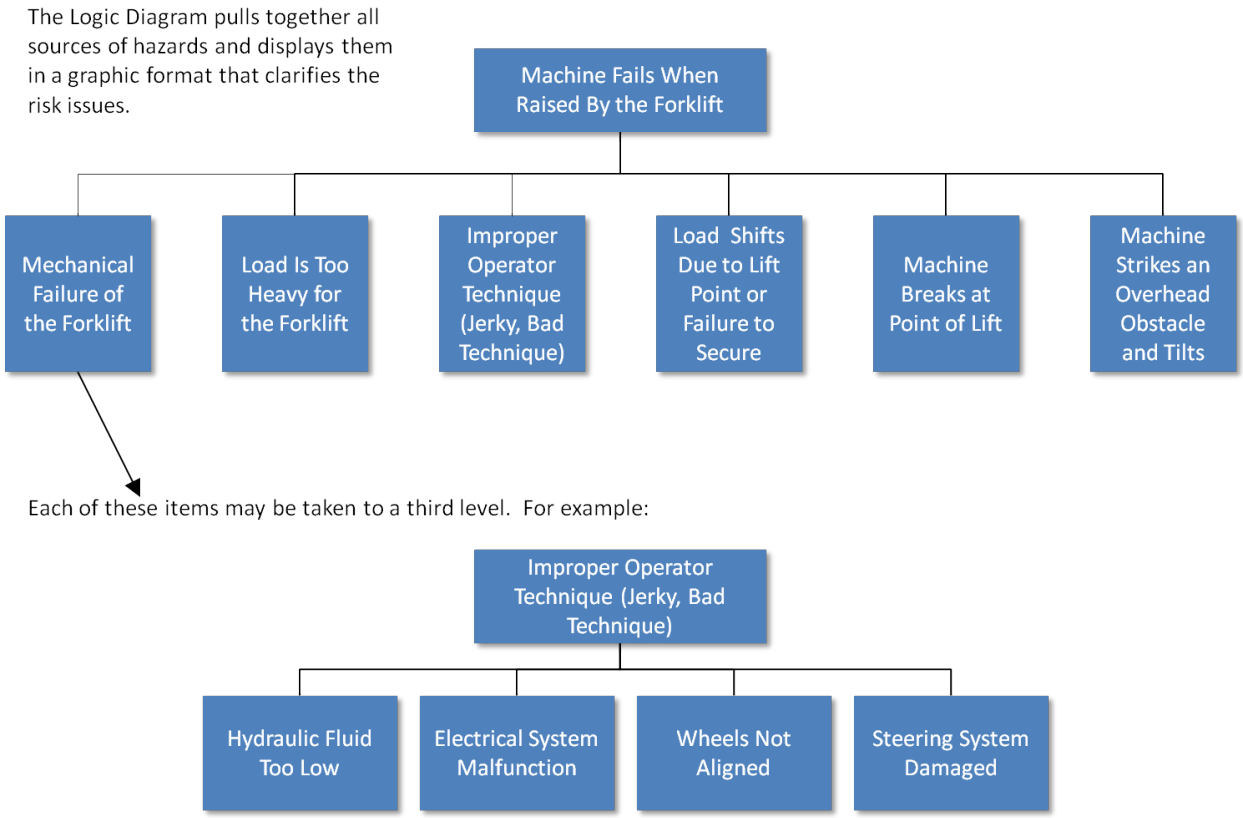


Figure C-13: Example Negative Diagram

C.2.22. Management Oversight and Risk Tree (MORT)

PURPOSE: 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 that might be present in an operation. 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 can be routinely used as a check on the 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: The full application of MORT is reserved for the highest risk 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, fills a book. There is an intermediate diagram with about 1,500 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.

COMMENTS: The MORT diagram is an elaborate negative Logic Diagram. The difference is primarily that the MORT diagram is already filled out for the user, allowing a person to identify the contributory factors for a given undesirable event. Since the MORT is very detailed, as mentioned above, a person can identify basic causes for essentially any type of event.

EXAMPLES: The top blocks of the MORT diagram are displayed below.

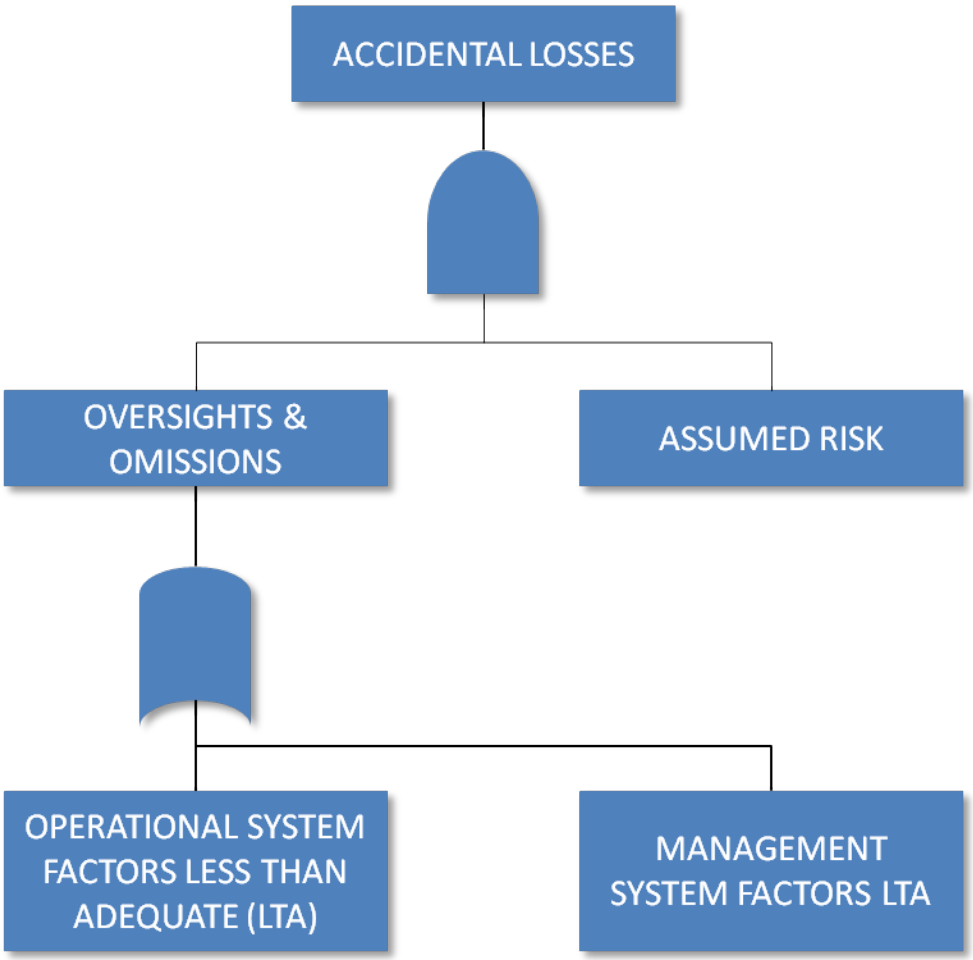


Figure C-14: Example MORT Section

C.2.23. Mapping Tool

ALTERNATIVE NAMES: Map analysis

PURPOSE: The Mapping Tool is designed 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 (e.g., 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. Then, 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 hazards involve the unwanted release of energy. The list below shows the kinds of energy to look for.

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)

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.

RESOURCES: Maps can convey a great deal of information but cannot replace the value of an on-site assessment. Similarly, when working with an equipment schematic or a facility layout, there is no substitute for an on-site inspection of the equipment or survey of the facility.

COMMENTS: The map analysis is valuable in itself, but it is also excellent input for many other tools such as the Interface Analysis, Energy Trace and Barrier Analysis, and Change Analysis.

EXAMPLE: The following example illustrates the use of a facility schematic that focuses on the energy sources that might be identified in support of an Energy Trace and Barrier Analysis.

SITUATION: A team has been assigned the task of renovating an older facility for use as a museum for historical aviation memorabilia. They evaluate the facility layout (schematic below). By evaluating the potential energy sources presented in this schematic, it is possible to identify hazards that may be created by the operations to be conducted.

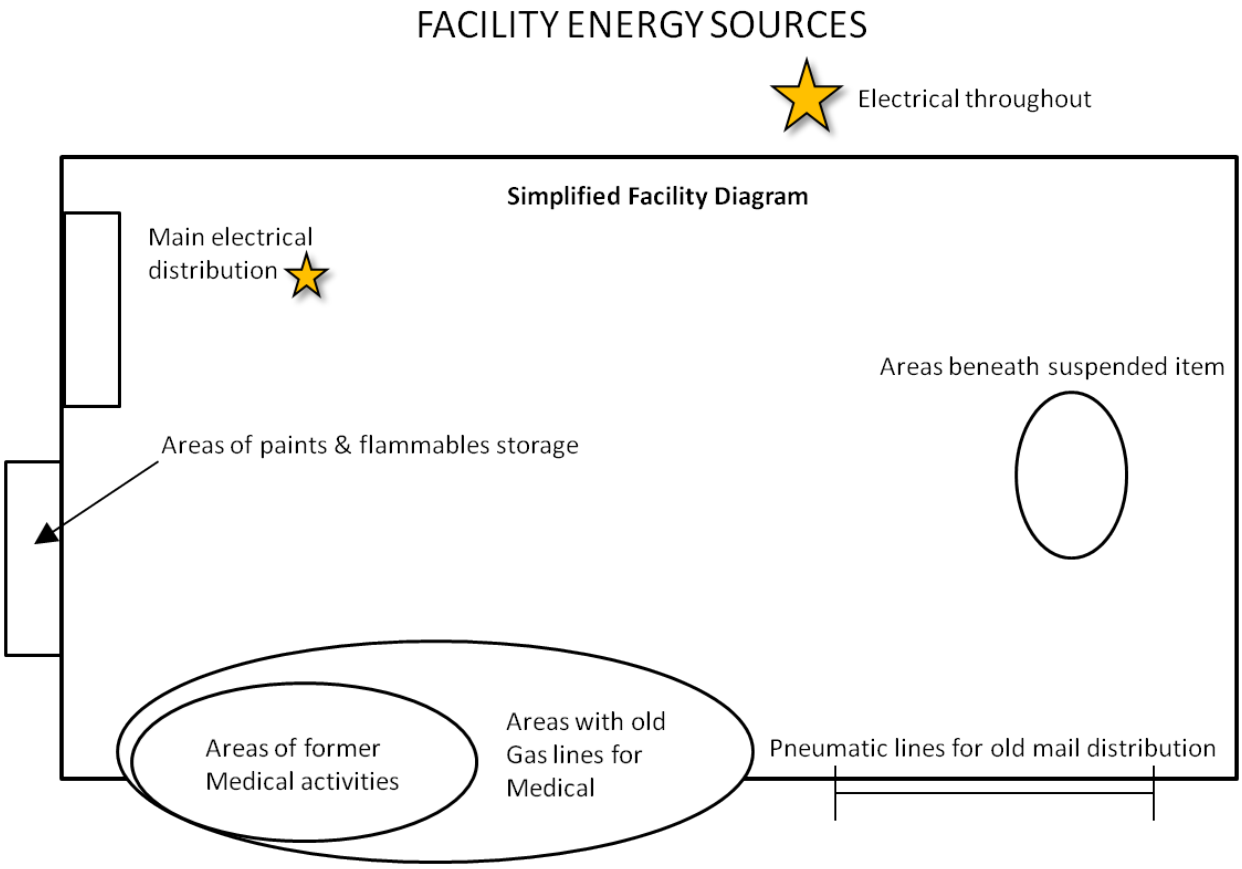


Figure C-15: Example Map Analysis

C.2.24. Monte Carlo Simulation

OVERVIEW: The Monte Carlo simulation uses repeated random sampling to estimate the expected number of future events (expected outcome) for specific problems as a function of specific operational and maintenance constraints. The simulation can also provide the percent of time a given number of events occurs in the simulated experience, which estimates the probability of actually seeing that particular outcome. Alternatively, the expected outcome can be used with the Poisson Distribution to calculate the probabilities. For example, the *expected* outcome might be 0.4 events, along with a 6% chance of *actually* having 2 or more events.

The simulation has as its inputs various distributions or values—failure distributions, inspection reliability, maintenance occurrences, utilization rate, equipment age—and samples from those distributions using random number generation over many repeated iterations. The simulation is typically a computer program that handles the sampling and calculations. The many iterations are simply repeat analyses within the computer program that simulate the behavior of the population under investigation (be it a certain fleet of airplanes or a certain type of equipment). Each iteration is a complete *simulated* experience; in real life, of course, only one *actual* experience will occur. The advantage of using simulation is that it provides the expected and possible outcomes much easier than is possible deterministically.

Simulation is especially helpful when many input distributions are required to predict risk under a given mitigation scenario. Constraints may also be varied to examine various scenarios of actions and their timing (operational restrictions; inspection intervals; retirement age) for their effect on risk. Sensitivity analyses can be performed to examine the effect of unknown variables. The simulation can also be designed to predict resource requirements under the various scenarios.

METHOD: The behavior of a particular unit (whether an aircraft, a part, or a piece of equipment) during a particular iteration is randomly selected from the distributions associated with the different inputs. The random selection can be thought of as many chances at rolling the dice or spinning the wheel (hence the “Monte Carlo” moniker) which, when summed together, give possible outcomes with their likelihood of occurrence. These results of repeated iterations are averaged to yield the expected outcome.

The goals of a simulation for an operational issue are to optimize the timing of mitigation actions and minimize the operational impact while identifying programs that achieve an acceptable level of risk reduction. The simulation should be calibrated to reproduce actual experience to date before being used to predict future experience.

RESOURCES: Simulations are typically programmed in computer language. If the analyst is adept at Microsoft Excel™, Excel can be used to ‘program’ a simulation through the use of macros and statistical functions. The analyst should attempt this only if they have familiarity with macros and the functions that will be required.

EXAMPLE: This example is not computer code but is rather an explanation of how the simulation uses random sampling in many repeated iterations to arrive at the expected outcome. This particular example explains the input distributions for the simulation of an engine part that can crack in service and propagate to failure, resulting in a flight-safety threat. The part is inspected for cracks at regular (varying) intervals and has a current mandatory retirement age not to exceed 15,000 cycles. The simulation is designed to estimate the expected number of failures. There are 1,000 parts in the suspect population. Though this example uses 100 iterations, typically, at least 1,000 or 10,000 iterations are performed to assure stability in the results.

In each iteration, each input distribution must be randomly sampled to give a simulated value for each engine part. The probability of a given value is determined by the random numbers assigned to that value. The random numbers are assigned based on the percent of the population failing vs. time. The following Weibull distribution for crack initiation has been developed from actual inspections and findings. Random sampling to select the time at which each part will crack first requires translating the Weibull distribution to the series of random numbers between 0 and 1.000. Bx.x life is the age at which x.x% of the population will fail (or, in this case, initiate a crack).

Weibull distribution		Random number
B0.01 initiation life	2,000 cycles	0.000
B0.1	3,000 cycles	0.001
B1.0	7,000 cycles	0.010
B6.0	11,000 cycles	0.060
etc.		
B99.9	35,000 cycles	0.999
B99.99	50,000 cycles	1.000

Now that the distribution has been translated to random numbers, the simulation is ready to sample the distribution. The simulation uses a random number generator to randomly select a number between 0 and 1. For example, the random number for part #1 in iteration #1 turns out to be 0.045. The simulation looks at the distribution that has been entered above and determines that 0.045 falls between 7,000 and 11,000 cycles initiation life. It then interpolates between those two lives with the same ratio as between their respective random numbers – in this case:

$$[(0.045 – 0.010) / (0.060 – 0.010)] = [(X – 7000) / (11000 – 7000)]$$

Solving for X gives an initiation life of 9,800 cycles.

The set of corresponding lives and random number probabilities is sometimes called pairwise points.

This process is repeated to calculate an initiation life for each part in the fleet, providing a distribution of initiation lives that should mirror the input distribution. A similar process is performed for crack propagation, age at inspection, and any other variable inputs, all based on their respective distributions. In this example, the simulation samples an initiation life, propagation life, inspection interval(s), and retirement age. The question of whether that particular part fails is then simply a matter of looking at whether it is retired, or its crack is found, prior to the sum of its initiation and propagation. For example:

Part #1, currently 7,000 cycles old *(actual age)*
Crack initiation life 9,800 cycles *(simulated)*
Propagation life 2,500 cycles (so, part fractures at 12,300 cycles) *(simulated)*
Failure = initiation + propagation = 9,800 + 2,500 = 12,300
On-wing inspections: 8,000 cycles – no crack found (none there yet) *(simulated)*
10,115 cycles – crack not found (based on inspection reliability distribution) *(simulated)*
Shop visit at 12,000 cycles *(simulated)*; part replaced – therefore, part does not fail, as it is scrapped prior to the point at which it fractures.

Part #2, currently 11,254 cycles old *(actual age)*
Crack initiation life 7,714 cycles *(simulated)*
Propagation life 4,400 cycles (part fractures at 12,114 cycles) *(simulated)*
On-wing inspections: 13,000 cycles *(simulated)*
Part fails prior to first inspection.

Part #3, currently 6,050 cycles old *(actual age)*
Crack initiation life 5,507 cycles *(simulated)*
Propagation life 4,216 cycles (part fractures at 9,723 cycles) *(simulated)*
On-wing inspections: 9,013 cycles – crack found *(simulated)*
Engine removed due to crack find – part does not fail.

This is repeated for all the parts in the population in each iteration. The entire 1,000 parts are then simulated anew in subsequent iterations. After all the iterations are complete, the simulation will average the results, giving the expected outcome.

For example: 1,000 parts – 100 iterations

40 iterations had 0 failures
53 iterations had 1 failure
6 iterations had 2 failures
1 iteration had 3 failures

total number of failures = (40 x 0) + (53 x 1) + (6 x 2) + (1 x 3) = 68
average number of failures = 68 / 100 iterations = 0.68

The expected outcome for the particular scenario used in this simulation is thus 0.68. The constraints for inspection and retirement can be varied and the same simulation program used again to estimate expected outcomes under the different scenarios.

C.2.25. Multi-Linear Events Sequencing Tool (MES)

ALTERNATIVE NAMES: The timeline tool, the sequential time event plot (STEP)[30]

PURPOSE: The Multi-Linear Events Sequencing Tool (MES) is a specialized hazard identification procedure designed 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 the person or equipment cannot be in two places at once. The MES can be used as a hazard identification tool or as an incident 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, especially when time relationships are relatively complex.

[30] K. Hendrisk, and L. Benner, Investigating Accidents with Step, Marcel Dekker, New York, 1988.

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, showing 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.

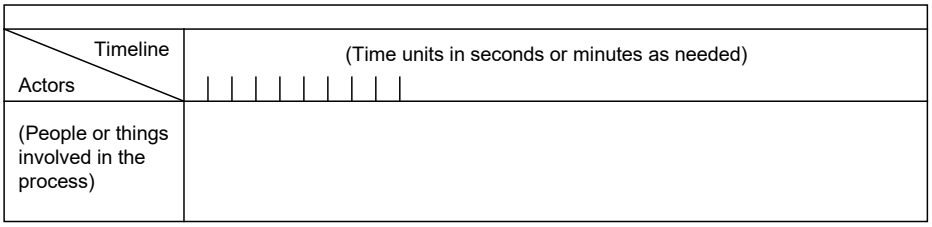


Figure C-16: Multi-Linear Events Sequencing Form

COMMENTS: The MES is unique in its role of examining the time-risk implications of operations.

C.2.26. Operating and Support Hazard Analysis (O&SHA)

OVERVIEW: The Operating and Support Hazard Analysis (O&SHA) is performed primarily to identify and evaluate the hazards associated with the environment, personnel, procedures, operation, support, and equipment involved throughout the total life cycle of a system/element. The O&SHA may be performed on such activities as testing, installation, modification, maintenance, support, transportation, ground servicing, storage, operations, emergency escape, egress, rescue, post-accident responses, and training. The O&SHA may also be selectively applied to facilities acquisition projects to make sure operation and maintenance manuals properly address safety and health requirements. The figure below shows O&SHA elements.

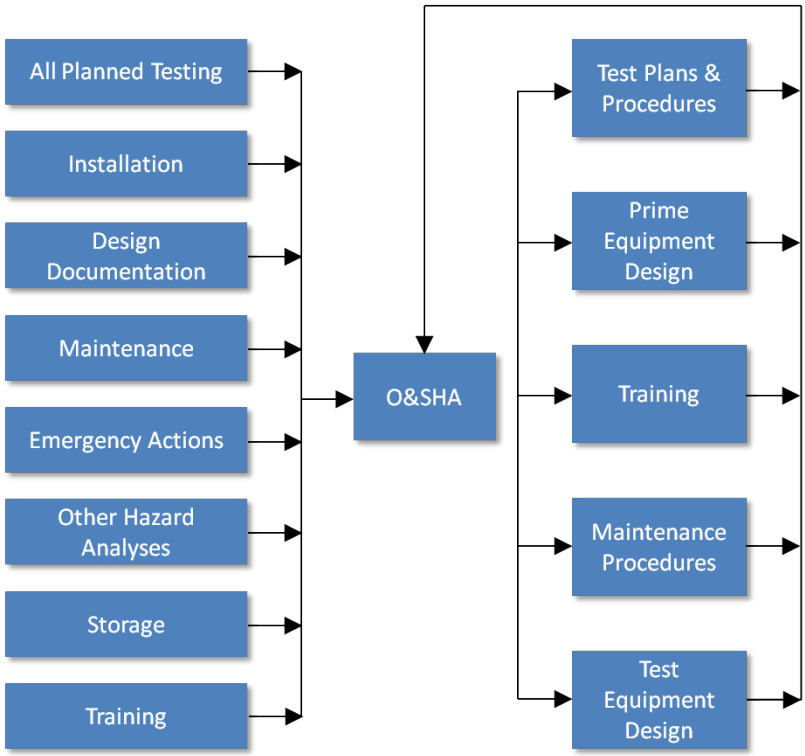


Figure C-17: Operating & Support Hazard Analysis (O&SHA) Elements

The O&SHA effort should start early enough to provide inputs to the design, system test, and operation. This analysis is most effective as a continuing closed loop iterative process, whereby proposed changes, additions, and formulation of functional activities are evaluated for safety considerations prior to formal acceptance. The analyst performing the O&SHA should have available:

- Engineering descriptions of the proposed system, support equipment, and facilities
- Draft procedures and preliminary operating manuals
- Preliminary Hazard Analysis (PHA), Subsystem Hazard Analysis (SSHA), and System Hazard Analysis (SHA) reports
- Related and constraint requirements and personnel capabilities
- Human factors engineering data and reports
- Lessons learned, including a history of accidents caused by human error
- Effects of off-the-shelf hardware and software across the interface with other system components or sub-systems

Timely application of the O&SHA will provide design guidance. The findings and recommendations resulting from the O&SHA may affect the diverse functional responsibilities associated with a given program. Therefore, it is important that the analysis results are properly distributed for the effective accomplishment of the O&SHA objectives. The techniques used to perform this analysis must be carefully selected to minimize problems in integrating O&SHAs with other hazard analyses. The O&SHA may be documented in any format that provides clear and concise information to the non-safety community.

The O&SHA identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons considering the following:

- Planned system configuration/state at each phase of activity
- Facility interfaces
- Planned environments (or ranges thereof)
- Supporting tools or other equipment, including software controlled automatic test equipment, specified for use
- Operational/task sequence, concurrent task effects and limitations
- Biotechnological factors, regulatory or contractually specified personnel safety and health requirements
- Potential for unplanned events, including hazards introduced by human error

The O&SHA must identify the safety requirements or alternatives needed to eliminate identified hazards, or to reduce the associated risk to a level that is acceptable under either regulatory or contractually specified criteria. The analysis may identify the following:

- Activities that occur under hazardous conditions, their time periods, and the actions required to minimize risk during these activities/time periods
- Changes needed in functional or design requirements for system hardware/software, facilities, tooling, or support/test equipment to eliminate hazards or reduce associated risks
- Requirements for safety devices and equipment, including personnel safety and life support equipment
- Warnings, cautions, and special emergency procedures (e.g., egress, rescue, escape), including those necessitated by failure of a software-controlled operation to produce the expected and required safe result or indication

- Requirements for handling, storage, transportation, maintenance, and disposal of hazardous materials
- Requirements for safety training and personnel certification

The O&SHA documents system safety assessment of procedures involved in system production, deployment, installation, assembly, test, operation, maintenance, servicing, transportation, storage, modification, and disposal. The O&SHA must be updated when needed as a result of any system design or operational changes.

Refer to ATO's Safety Risk Management Guidance for System Acquisitions document for new acquisitions where the Acquisition Management System applies.

C.2.27. Operational Safety Assessment (OSA)

OVERVIEW: The OSA is a development tool based on the assessment of hazard severity. It establishes how safety requirements are to be allocated between air and ground components and how performance and interoperability requirements might be influenced. The OSA provides the system designers and management with a set of safety goals for design. It provides an environment description and a Preliminary Hazard List (PHL) for a given proposal or design change. The OSA assesses the potential severity of the hazards listed in the PHL. These severity codes are then mapped to a preset level of probabilities, which establishes the safety objectives for controlling the hazard. For instance, a catastrophic hazard would be mapped to a probability requirement that is more stringent than a minor hazard. This process establishes the safety target level for controlling the hazard. This target level, or goal, assists in the establishment of safety requirements for the system design.

The OSA is composed of three fundamental elements: (1) the Operational Services and Environment Description (OSED), (2) an Operational Hazard Assessment (OHA), and (3) an Allocation of Safety Objectives and Requirements (ASOR).

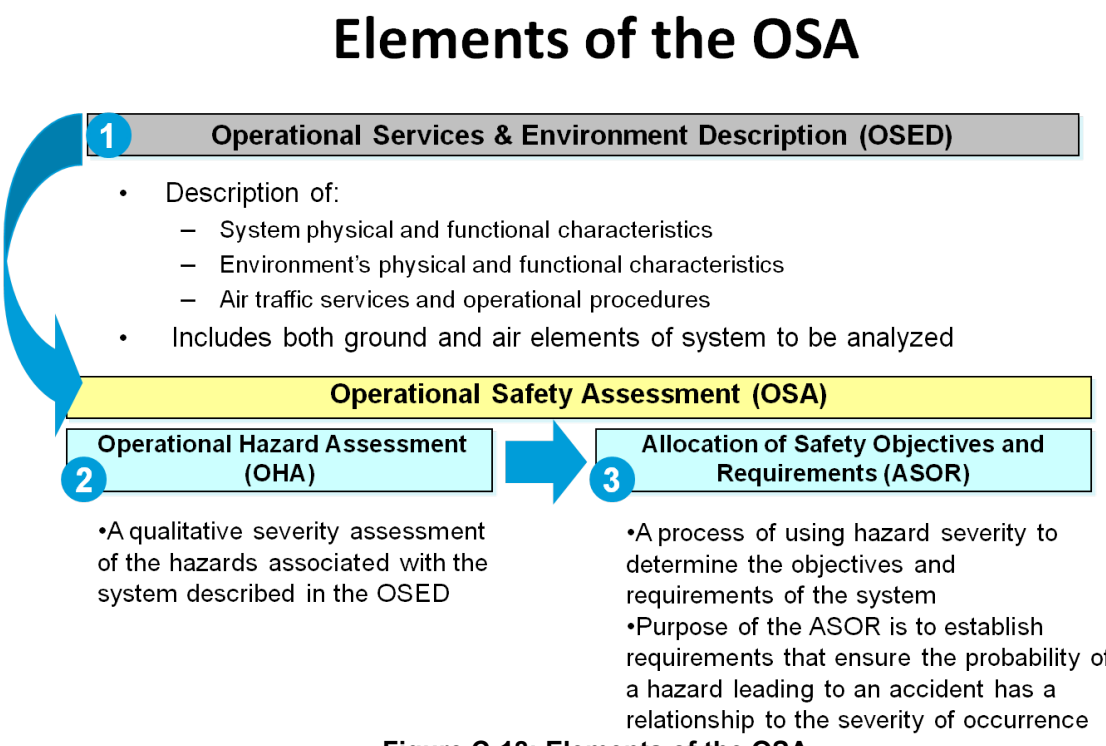


Figure C-18: Elements of the OSA

The OSED is a description of the system physical and functional characteristics; the environment's physical and functional characteristics; and air traffic services and operational procedures. This description includes both the ground and air elements of the system to be analyzed. The OHA is a qualitative safety assessment of the operational hazards associated with the OSED. Each hazard is classified according to its potential severity. Each classified hazard is then mapped to a safety objective based on probability of occurrence. In general, as severity increases, the safety objective is to decrease probability of occurrence.

The information contained in the OSA supports the early definition of system-level requirements. It is not a risk assessment in a classical sense. Instead, the OSA's function is to determine the system's requirements early in the life cycle. The early identification and documentation of these requirements may improve system integration, lower developmental costs, and increase system performance and the probability of program success.

While the OSA itself is not a risk assessment, it does support further safety risk assessments that are required by FAA Order 8040.4, *Safety Risk Management Policy*. The follow-on safety assessments may build on the OSA's OSED and OHA by using the hazard list, system descriptions, and severity codes identified in the OSA. The OSA also provides an essential input into Comparative Safety Assessments (CSAs) that support trade studies and decision making in the operational and acquisition processes.

PROCESS: The OSA process is depicted below.

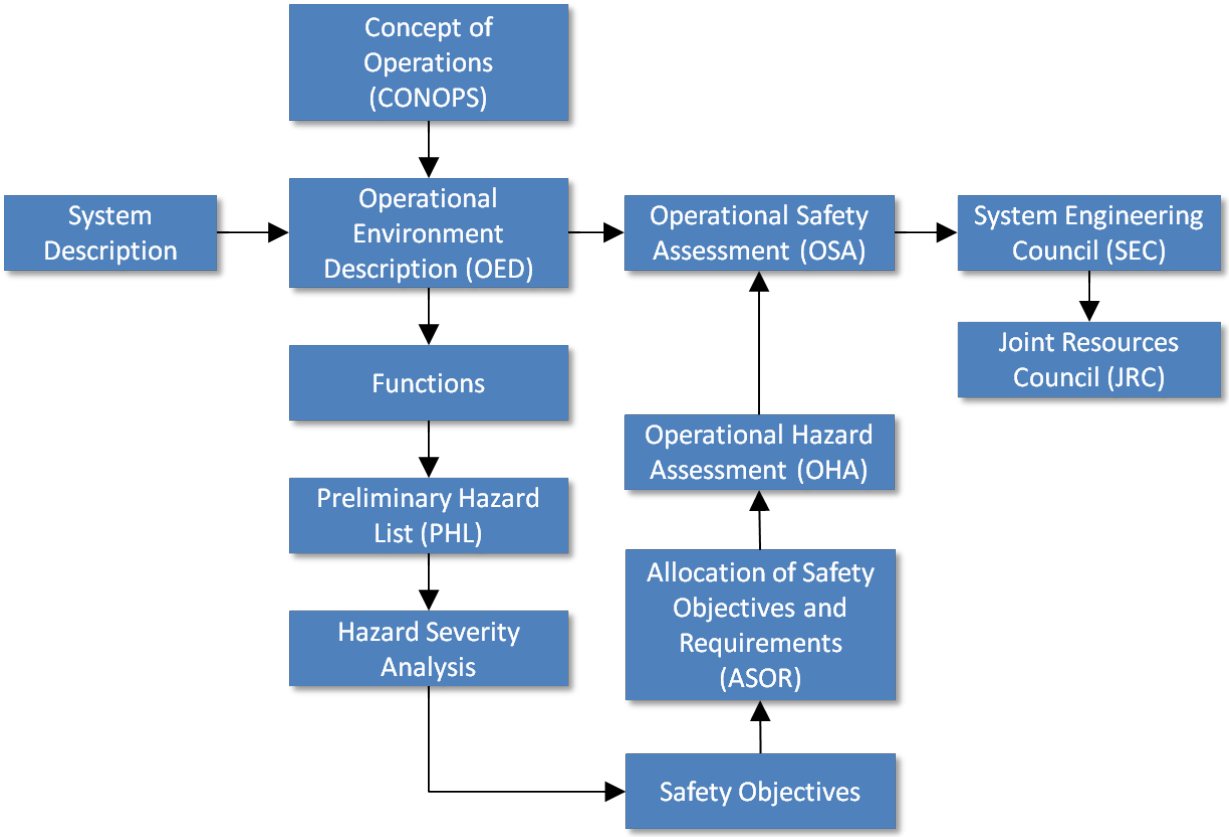


Figure C-19: OSA Process

C.2.27.1. Operational Services and Environment Description (OSED)

OVERVIEW: The Operational Services and Environment Description (OSED) is the first part of the Operational Safety Assessment (OSA). The OSED is basically a system description that may include all the elements of the 5M Model.

The OSED shall include as a minimum the following:

Functional description or architecture: This section describes the system boundaries, functions, and functional architecture in accordance with functional analysis.

Procedures: This section describes the existing and new procedures and policies that govern the system's operation or maintenance to include:

- Operational requirements and regulations, including separation minima
- Deployment requirements
- Operational scenarios

Human elements of the system: This section describes the operators and maintainers of the system, including information regarding:

- Anthropometric requirements
- Training requirements
- Specific skill set requirements
- Human-system integration requirements

Equipment and software: This section describes any known hardware and software that is required for system operation. This section, in particular, may not be appropriate in the early stages of development.

Environmental description: This section is an expression of the various conditions in which the system is operated, including:

- Operational: The operational environment includes factors such as traffic density and flow, flight phases, traffic complexity, route configuration, type of control, use of visual or instrument flight rules, etc.
- Ambient: The ambient conditions refer to visual and instrument meteorological conditions, altitudes, terrain elevations, and physical conditions, such as electromagnetic environment effects, precipitation, icing, etc.

Non-functional requirements: This section describes any other requirements that are not covered in other sections and includes, but are not limited to, the following:

- Time constraints
- Information exchanges
- Exception handling

C.2.27.2. Operational Hazard Analysis (OHA)

OVERVIEW: The Operational Hazard Assessment (OHA) is the second part of the Operational Safety Assessment (OSA). The OHA is a qualitative assessment of the hazards associated with the system described in the Operational Services and Environment Description (OSED).

The OHA includes tabular work sheets and the Preliminary Hazard List (PHL). Once the system has been bounded, described, and the functions determined in the OSED, the analyst or SRM Team is ready to determine the hazards associated with the system. For these types of assessments, the best method is to assess scenarios containing a set of hazardous conditions.

Since the work has already been done in defining the system operational environment, it is often best to relate the functions of the system to hazards. For example, in analyzing the NAS, one would find the following functions of the NAS.

Table C-3: Examples of NAS System Functions and Their Associated Hazards

NAS System Function	NAS System Hazard
Provide air – ground voice communications	No air – ground voice communication
Provide precision approach instrument guidance to runways	No precision instrument guidance to the runway
Provide En Route Flight Advisory Service (EFAS) of severe weather	EFAS warning of severe weather in flight path to CSA flight crew not received

These functions are then translated into hazards that would be included in the PHL. For many of the listed hazards, other conditions must be present before an accident could occur. These are described in the detailed description of the risk assessment. The purpose here is to develop a concise, clear, and understandable PHL.

In addition to the functional analysis, the following tools can be used to identify the foreseeable hazards to the system operation:

- Operations Analysis
- "What If" Tool
- Scenario Process Tool
- Logic Diagram
- Change Analysis
- Cause and Effect Tool

From the function list, the analyst develops the list of hazards potentially existing in the system under study and determines the potential severity of each hazard in the hazard list.

C.2.27.3. Allocation of Safety Objectives and Requirements (ASOR)

OVERVIEW: The Allocation of Safety Objectives and Requirements (ASOR) is the process of using hazard severity to determine the safety objectives and requirements of a system. It establishes requirements ensuring that high probability hazards which may lead to an accident have low severity or consequence, whereas high severity hazards will have a low probability of occurrence.

The following objectives should be met for the ASOR:

- **Stakeholder identification:** The applicants, approval authorities, and stakeholders needed to establish and show compliance to requirements for the Air Traffic Services (ATS) provision, its use, and related Communication, Navigation, and Surveillance (CNS) or Air Traffic Management (ATM) system are identified.
- **Identification of system failure relationships:** Identify the relationships of CNS and ATM system failures, procedural errors, and the effects on air traffic services to the hazard. Include identification of common cause failures and errors occurring among elements of the system.
- **Identification of shared risk mitigation strategy:** Identify risk mitigation strategies that are shared by multiple elements of the CNS and ATM system, including mitigation from effects of common cause failures and errors occurring across system elements. CNS and ATM system mitigation includes architectural and procedural aspects of the system and environmental mitigation and related candidate safety requirements identified in the OHA.
- **Identification of safety requirements:** Determine safety requirements from the shared risk mitigation strategies that satisfy the safety objectives.
- **Allocation of Safety Objectives and Requirements:** Allocate the safety objectives and requirements, including requirements from environmental mitigation to elements of the CNS or ATM system.
- **Traceability of ASOR results to OHA:** Trace the ASOR results to each safety objective identified in the OHA.
- **Shared safety objective and requirement coordination:** Coordinate the ASOR results:
    - The impact of the ASOR on the NAS and other operational assessments are identified and reported.
    - The impact of the ASOR on development and qualification of solution elements is identified and reported to the appropriate organizations. This impact includes criteria for quantifying safety objectives, determining development assurance requirements, considering architecture (including design features), and reducing the effects of generic design and implementation errors. Criteria for validating the effectiveness of procedural requirements are also provided.
- **Validation of OSA results:** Ensure the correctness and completeness of the safety objectives and requirements, including candidate safety requirements identified during the OHA. This ensures that requirements are necessary and sufficient for operational implementation. The validation may include analysis, simulation evaluations, prototype testing, and operational trials. The validation includes a consistency check between the requirements and the OSED.

The following tasks are conducted in the ASOR Phase:

- Determine existing controls and safety requirements for each hazard,
- Develop those requirements based on the safety goals, and
- Allocate the requirements to either or both the ground CNS and ATM or airborne systems.

C.2.28. Operations Analysis (OA)

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

PURPOSE: The Operations Analysis (OA) provides 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 a major weakness of traditional risk management, which tends to focus effort 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 Operations Analysis 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 imagine planning an operation without identifying the key events in a time sequence. If for some reason such a list is not available, the analyst creates it using the best available understanding of the operation. The best practice is to break down the operation into time-sequenced segments strongly related 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.

An alternative to the OA is the flow diagram. Commonly used symbols are shown below.

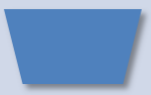
SYMBOL	REPRESENTS	EXAMPLE
	START	RECEIVE TASKING BEGIN TRIP OPEN CHECKLIST
	ACTIVITY	OPERATION PLANNING START CAR STEP ONE IN CHECKLIST
	DECISION POINT (OR)	YES/NO APPROVE/DISAPPROVE PASS/FAIL
	FORK/SPLIT (AND)	PREPOSITION VEHICLES AND SUPPLIES RELEASE CLUTCH AND PRESS ACCELERATOR OBSERVE FLIGHT CONTROLS WHILE MOVING STICK
	END	FINAL REPORT ARRIVE AT DESTINATION AIRCRAFT ACCEPTED

Figure C-20: Example Flow Chart Symbols

Putting the steps of the process on index cards or adhesive notes allows the diagram to be rearranged without erasing and redrawing, thus encouraging contributions.

RESOURCES: The key resource for the OA is the operational planners. Using their operational layout will facilitate the integration of risk controls in the main operational plan and will eliminate the expenditure of duplicate resources on this aspect of hazard identification.

EXAMPLE: If more detail and more structured examination of the operational flow are desired, the flow diagram can be used. This diagram will add information through the use of graphic symbols. A flow diagram of the planning phase might be developed as illustrated below.

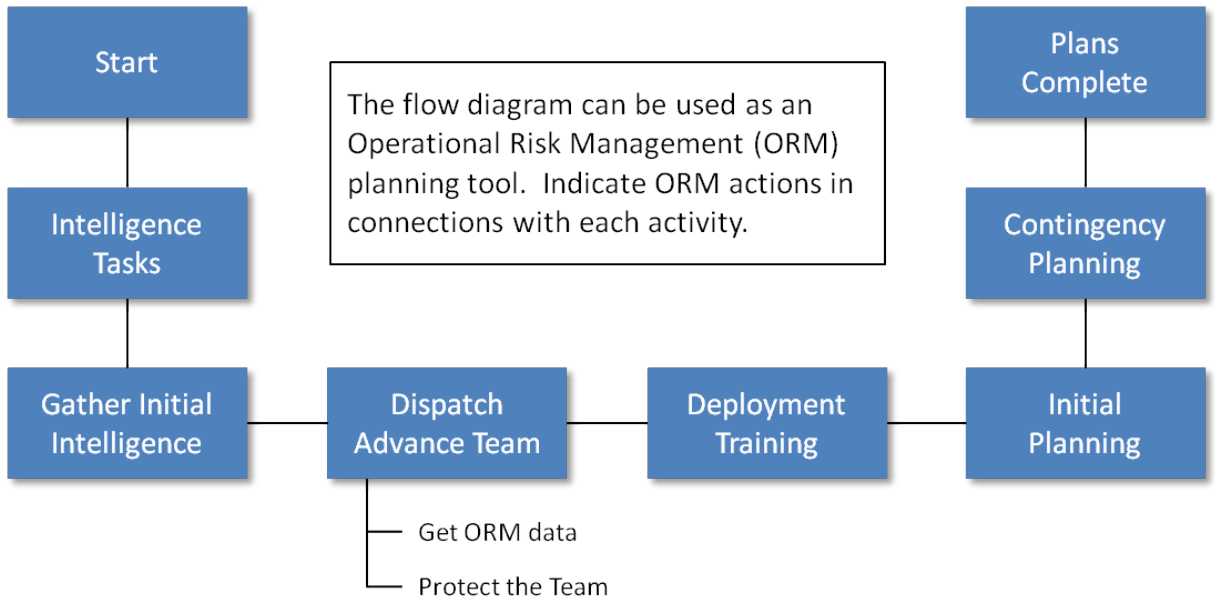


Figure C-21: Example Flow Diagram

C.2.29. Poisson Distribution

OVERVIEW: The Poisson distribution is used to model data that occurs as discrete events within a given period of time or distance. Examples include the number of defects in production lots or the number of In-Flight Shutdowns (IFSDs) that occur in a given day. The possible number of occurrences may be much larger than the average, and the events are independent of each other. The Poisson distribution has applicability to the risk assessment process in that it is used to calculate the probability of a particular number of events ('k') for a predicted average outcome. Typically, we are interested in the probability of getting k *or more* events.

METHOD: The relevant parameter for the Poisson distribution is *lambda* (λ), or the expected outcome. A risk analysis may predict 0.5 additional failures. This actual outcome—a fraction of a failure or event—is not possible. Using the Poisson, probabilities of actually getting a particular number of failures can be calculated (see example for calculations). The formula for this is then:

$$\Pr(k \text{ failures}) = (\lambda^k * e^{-\lambda}) / k!$$

In this example, λ is 0.5. Probabilities of *at least* k events are obtained by summing the results for all (k-1) values and subtracting that sum from 100%.

RESOURCES: Poisson values may be read directly off Poisson tables available in statistics textbooks or online. Interpolation may be necessary. Microsoft Excel™ has several functions

that will calculate exact Poisson values. Caution is urged that the analyst not use these functions without a thorough understanding of the Poisson distribution and its applications. Some functions will return the probability of the exact number of failures (k); others will return the probability of at least k failures.

EXAMPLE: From the formula above, an expected outcome (λ) of 0.5 predicted additional events translates to probabilities of:

k	Exactly k events	k or more events	
0	60.7%	-	
1	30.3%	39.3%	(100 - 60.7)
2	7.6%	9.0%	(100 - 60.7 - 30.3)
3	1.3%	1.4%	(100 - 60.7 - 30.3 - 7.6)
4	0.2%	0.2%	(100 - 60.7 - 30.3 - 7.6 - 1.3)*
etc.			*rounding error

C.2.30. Preliminary Hazard Analysis (PHA)

PURPOSE: The Preliminary Hazard Analysis (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. The key idea of the PHA is to consider the risk inherent to every aspect of an operation. 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. The PHA is used in the System Hazard Analysis (SHA) and the Subsystem Hazard Analysis (SSHA).

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 as shown below.

Building the PHA Directly From the Operations Analysis Flow Diagram

Operational Phase Hazards

List the operational phases vertically down the page. Be sure to leave plenty of space on the worksheet between each phase to allow several hazards to be noted for each phase.	List the hazards noted for each operational phase here. Strive for detail within the limits imposed by the time you have set aside for this tool.

Alternatively, a more formal PHA format such as the worksheet shown below can be used.

Example 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 direct 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	– 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	– Forklift strikes the machine – Forklift strikes other items in the area
Lift the machine	– 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	– Instability due to rough surface or weather condition – Operator error causes load instability – The load shifts
Place machine on the truck	– Improper tiedown produces instability – Truck overloaded or improper load distribution
Drive truck to building B	– Vehicle accident during the move – Poor driving technique produces instability – Instability due to road condition
Remove machine from the truck	– Same factors as “Move it to the truck”
Place machine in proper position in building B	– Same factors as “Raise the machine” except focused on lowering the machine

The completed PHA is used to identify hazards requiring more in-depth hazard identification or it may lead directly to the remaining five steps of the SRM process if hazard levels are judged to be low. Key to the effectiveness of the PHA is assuring that all events of the operation are covered.

RESOURCES: The two key resources for the PHA are the expertise of personnel actually experienced in the operation and the body of regulations, standards, and instructions that may be available. The PHA can be accomplished in small groups. List the operational phases vertically down the page. Be sure to leave plenty of space on the worksheet between each phase to allow several hazards to be noted for each phase. 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 significant power to impact risk arises from the forced consideration of risk in all phases of an operation. This means that a key to success is to link the PHA closely to the Operations Analysis.

C.2.31. Preliminary Hazard List (PHL)

As its name supports, the Preliminary Hazard List (PHL) is simply a first cut list of hazards. Before the SRM Team convenes, the facilitator and OPR may develop an initial PHL. To expand on this initial PHL and reveal hazards that were not previously identified, the SRM Team should hold a brainstorming session where ideas are put to paper (see the "What If" Tool). Once the brainstorming session is over, the list will be a combination of hazards, causes, effects, and system states. The facilitator can work with the SRM Team in reviewing the list and categorizing each item. The resulting hazards, causes, effects, system states, etc., will then be worked into a PHA or HAW.

C.2.32. Root Cause Analysis (RCA)

ALTERNATIVE NAMES: Apollo Root Cause Analysis

OVERVIEW: The Apollo Root Cause Analysis (RCA)[31] is a method of problem solving that is designed to be applied after an incident as a means to identify root causes that can be mitigated or eliminated from recurring. Though it uses reactive data collection methods, it is actually a proactive prevention technique.

RCA is basically a step-by-step process for how to use the Fault Tree Analysis (FTA). RCA starts with the primary effect or problem and begins the tree by asking for the immediate cause of that primary effect. Each effect was caused by at least one of each of the two types of causes—action causes and condition causes. (These are equivalent to hazards and system states described in the ATO SMS Manual.) The fault tree can continue with more causes by branches until the causes are broken down to the most elementary level or more information is needed.

Solutions are generated for every cause in a brainstorming session. As long as the solution meets certain criteria, the merit of each solution is not weighed at this point. It is simply an idea-generating exercise. After solutions are identified for each cause, the process of finding the best solution(s) begins.

METHOD: The process is broken up into four steps: Define the Problem, Create a Cause and Effect Chart, Identify Effective Solutions, and Implement the Best Solutions.

Step 1: Define the Problem

The RCA method describes how important this first step is in the problem-solving process. The more specific the problem definition, the easier it will be to identify effective solutions. It is also important to understand the importance of perspective in a problem definition. From an Air Traffic Safety Inspector's (ATSI) perspective, the problem with a runway incursion may be the fact that the safety of the public was threatened. The airline's concerns may be more economical in that an accident could be very costly—the cost to repair the airplane, loss of future revenue from weary flyers, worker's compensation for employees, medical costs for passengers, and possible legal costs. The pilot or controller may be concerned about losing his or her job if the runway incursion was a result of poor job performance. Every side involved may wish that the runway incursion did not occur, but from different perspectives that may steer the RCA process in different directions.

[31] D.L. Gano, Apollo Root Cause Analysis: A New Way of Thinking, Apollonian Publications, 2007.

There are four elements to a problem definition:

- **What:** The “what” is the primary effect that we want to keep from recurring and the point at which we begin asking why (e.g., Pilot Deviation).
- **When:** The “when” should consist of both chronological timing (12/22/08 at 0300 Zulu) and relative timing (at night, during a thunderstorm, winds 15-25kts at 150) which can help formulate the why questions. Knowing an incursion happened at night might indicate a tired controller or pilot.
- **Where:** The “where” should also combine specific location information (LAS, intersection of runways 19L and 25R) as well as the relative location (altitude and weather).
- **Significance:** Defining the significance will help determine how much time should be spent on the problem, what types of people/specialties will make up the team working on the problem, and why the problem needs to be worked in the first place.

Step 2: Create a Cause and Effect Chart

There are four characteristics of the Cause and Effect Principle:

- **First:** The effect of one event can be the cause of a subsequent event as illustrated in Figure C-22 below:

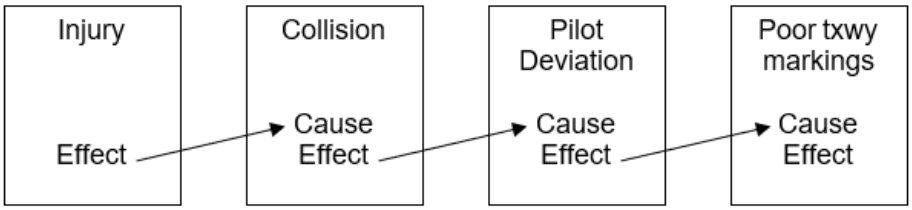


Figure C-22: Cause and Effect Relationship

- **Second:** Causes and Effects are part of an infinite continuum. Causes and effects often connect in several ways because they are always part of a bigger picture. However, the more connections, the better this bigger picture becomes and the easier it is to determine the root cause. Individually, they can be the beginning or the end. The Pilot Deviation could have been caused by the poor taxiway markings, but why are the markings poor or hard to read?
- **Third:** Each Effect has at least two Causes in the form of Actions and Conditions. This idea is similar to the ATO SMS relationship of hazards and system states. In the Apollo RCA method, an action cause is the same as a hazard and can usually be described in two words in a noun-verb format (e.g., Pilot Deviated). Likewise, condition causes are the same as system states (e.g., instrument meteorological conditions [IMC]).

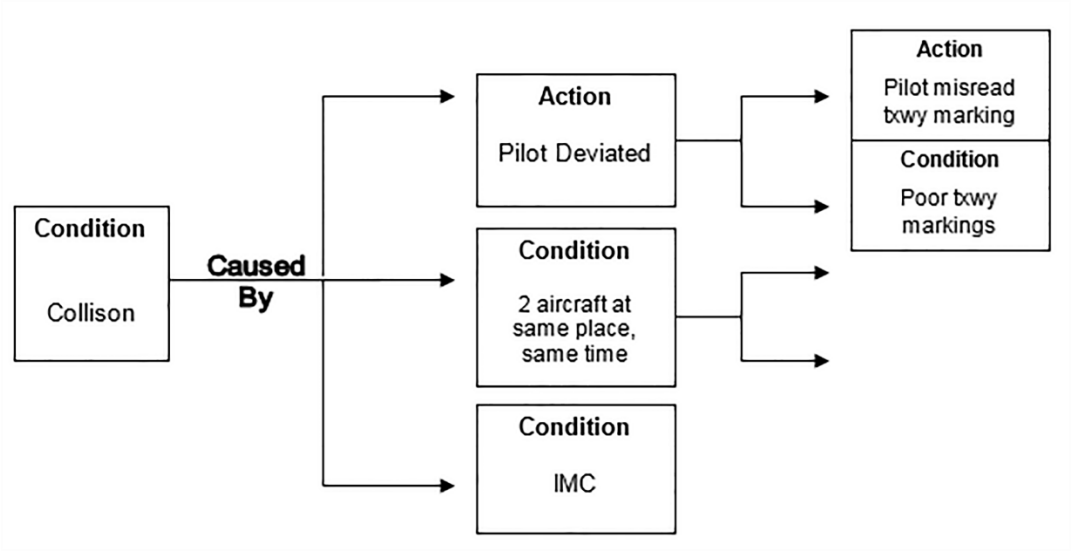


Figure C-23: Conditions and Actions

- **Fourth:** An Effect exists only if its Causes exist. The causes of any effect must exist at the same time and place before the effect can exist. This is a simple check to validate your cause and effect relationships. If you remove a cause and the effect remains, it does not belong in the causal set.

Step 3: Identify Effective Solutions

The author of the *Apollo Root Cause Analysis: A New Way of Thinking* explains here, "it is not the root causes we seek, it is effective solutions." This means that once we have discovered the root cause or causes (there can be more than one), we are not any better off unless we can come up with effective solutions to mitigate those causes.

This is the point in the RCA method where it benefits the Team to have made a very detailed cause and effect chart. The team now looks at its chart and comes up with solutions to every single cause. There are several criteria for solutions. They must:

- **Prevent recurrence.** Solutions must prevent or mitigate the problem or similar problems and they must not create additional problems or unacceptable situations.
- **Be within your control.** Your control may be you, your department, your company, your suppliers, or your customers.
- **Meet your goals and objectives.** These could be goals of your department or your overall organization (i.e., Aviation Safety [AVS] commitment to safety, ATO SMS).

During the process of identifying solutions, it is very important to be creative and not restrict any ideas. This is the big brainstorming portion of the RCA method, and it is important that all possible ideas are written down before anything is ruled out.

Apollo identifies some "solution killers" that should be avoided during this solution generating process:

- It will never work here.
- We're too busy to do that.
- No one will buy it.

- We already tried that once.
- That's not our policy here.
- It isn't in the budget.
- Good thought, but impractical.
- Top management will never go for it.
- No one else is doing it that way.
- We've always done it that way.
- Good idea. I'll get back to you—and never does.
- We will just be extra careful in the future.

Step 4: Implement the Best Solutions

After solutions to each cause are identified, it is time to implement the best solution(s). Deciding on the best solution is, again, a question of perspective. The above criteria for effective solutions (prevent recurrence, are within your control, and meet your goals and objectives) must all be met. It is in the third criterion, meeting goals and expectations, where perspective comes into play. As an ATSI, you might opt for the solution that achieves the highest possible level of safety. As an airline, however, you may choose the most cost-effective solution.

Apollo offers some helpful hints for this process. A hint that stands out is:

- **Look for the Systemic Solution.** Avoid solutions that include the prefix "re," for example, retrain, re-read, replace.

Though it is important that controllers receive refresher training, Apollo argues that retraining cannot be the only solution and that certain questions must be asked if this is the case. Why do controllers need refresher training? What was wrong with the training the first time?

Other Tips

Apollo offers other helpful hints for making this process as effective as possible.

- **Avoid placing blame.** If the solution is to punish or place blame, make sure it will prevent recurrence.
- **Solutions should be specific actions.** Do not include solutions that are to be carried out in the future, such as "review…," or "analyze…," or "investigate…" These are indicative of an incomplete problem analysis.
- **Sometimes there are no clear solutions.** Devise a plan to capture more causal evidence if it happens again and implement interim solutions that will mitigate the consequences.

C.2.33. Scenario Process Tool

ALTERNATIVE NAMES: The mental movie tool

PURPOSE: The Scenario Process tool is a time-tested procedure 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 to 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 can 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. It is often effective to close the eyes, relax, and let the images flow. Usually, the best procedure is to use the flow of events established in the Operations Analysis (OA). An effective method is to visualize the flow of events twice. The first time, see the events as they are intended to flow. The next time, inject “Murphy” at every possible turn to see what could go wrong. As hazards are visualized, they are recorded for further action. Some good guidelines for the development of scenarios are as follows:

- Limit them to 60 words or less.
- Don’t 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.

RESOURCES: The key resource for the Scenario Process tool is the OA. It provides the script for the flow of events that will be visualized. Using the tool does not require a specialist. Operational personnel leading or actually performing the task being assessed are key resources for the OA.

COMMENTS: A special value of the Scenario Process tool is its ability to link two or more individual hazards developed using other tools into an operation relevant scenario.

EXAMPLES: The following is an example of how the Scenario Process tool might be used in an operational situation.

Example Machine Movement Scenario

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

C.2.34. Sneak Circuit Analysis

OVERVIEW: The Sneak Circuit Analysis (SCA) is a unique method of evaluating electrical circuits. SCA employs recognition of topological patterns that are characteristic of all circuits and systems. The purpose of this analysis technique is to uncover latent (sneak) circuits and conditions that inhibit desired functions or cause undesired functions to occur, without a component having failed. An automobile circuit that contains a sneak circuit is shown below. The sneak path is through the directional switch and flasher, the brake light switch, and the radio.

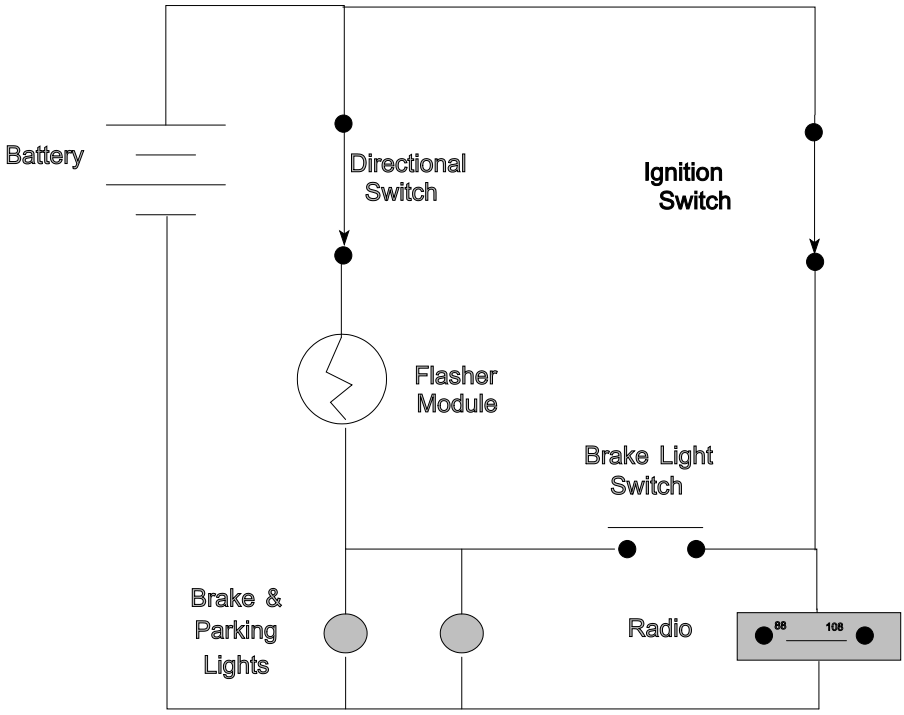


Figure C-24: A Sneak Circuit

The latent nature of sneak circuits and the realization that they are found in all types of electrical/electronic systems suggests that the application of SCA to any system that is required to operate with a high reliability is valuable. This process is quite expensive and is often limited to highly critical (from the safety viewpoint) systems. The tool has been successfully applied to nuclear plant safety sub-systems, ordnance handling systems, and space craft. Consideration should be given to utilizing this tool for FAA applications that eliminate human control such as an autopilot.

The fact that the circuits can be broken down into the patterns shown allows a series of clues to be applied for recognition of possible sneak circuit conditions. These clues help to identify combinations of controls and loads that are involved in all types of sneak circuits. Analysis of the node topographs for sneak circuit conditions is done systematically with the application of sneak circuit clues to one node at a time. When all the clues that apply to a particular pattern have been considered, it is assured that all possible sneak circuits that could result from that portion of the circuit have been identified. The clues help the analyst to determine the different ways a given circuit pattern can produce a “sneak.” A node topograph equivalent of the previous illustration follows.

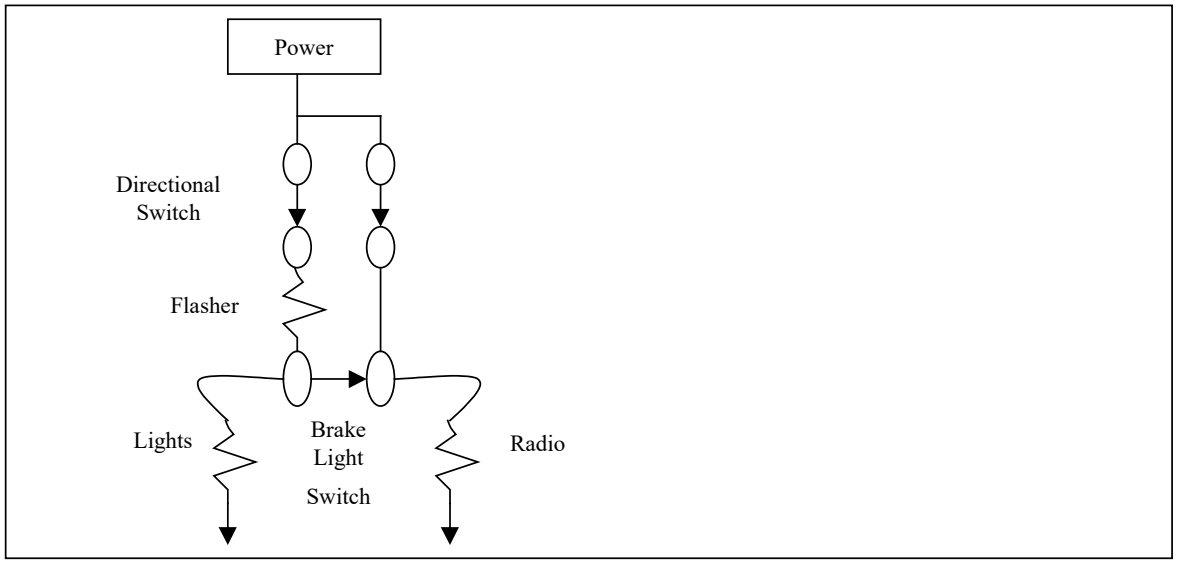


Figure C-25: Topical Node Representation of Sneak Circuit

There are four basic categories of sneak circuits that will be found.

- Sneak Paths - Allow current to flow along an unsuspected route
- Sneak Timing - Causes functions to be inhibited or to occur unexpectedly
- Sneak Labels - Cause incorrect stimuli to be initiated
- Sneak Indicators - Cause ambiguous or false displays

In addition to identification of sneak circuits, SCA also reveals design concerns (e.g., unnecessary components or lack of redundancy) and discrepancies within documentation referred to as drawing error conditions. Design concern conditions include:

- Unsuppressed or improperly suppressed inductive loads
- Excess or unnecessary components
- Lack of redundancy
- Failure points

The three resultant products of SCA (sneak circuit, design concern, and drawing error conditions) are reported with an explanation of the condition found, illustrated as necessary, and accompanied with a recommendation for correction.

C.2.35. Subsystem Hazard Analysis (SSHA)

OVERVIEW: In acquisitions, the general purpose of the SSHA is to perform a safety risk assessment of a system's sub-systems and components at a more detailed level than that provided in a Preliminary Hazard Analysis (PHA). The SSHA is performed if a system under development contains sub-systems or components that, when integrated, function together in a system. This analysis examines each sub-system or component and identifies hazards associated with normal or abnormal operations; it is intended to determine how operation or failure of components, or any other anomaly, adversely affects the overall safety of the system. This analysis should identify existing and recommended actions using the Safety Order of Precedence to determine how to eliminate or reduce the risk of identified hazards.

The SSHA is used to:

- Verify sub-system compliance with safety requirements contained in sub-system specifications and other applicable documents;
- Identify previously unidentified hazards associated with the design of sub-systems including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and equipment comprising each sub-system; and
- Recommend actions necessary to eliminate identified hazards and/or control their associated risk to acceptable levels.

The analysis should include a determination:

- Of the modes of failure including reasonable human errors as well as single point and common mode failures, and the effects on safety when failures occur in sub-system components;
- Of potential contribution of hardware and software (including that which is developed by other sources) events, faults, and occurrences (such as improper timing) on safety of the sub-system;
- That the safety design criteria in the hardware, software, and facilities specification(s) have been satisfied;
- That the method of implementation of the hardware, software, and facilities design requirements and corrective actions has not impaired or decreased the safety of the sub-system nor has it introduced any new hazards or risks;
- Of the implementation of safety design requirements from top level specifications to detailed design specifications for the sub-system (the implementation of safety design requirements developed as part of the PHA shall be analyzed to ensure that it satisfies the intent of the requirements);
- Of test plan and procedure recommendations to integrated safety testing into the hardware and software test programs; and
- That system level hazards attributed to the sub-system are analyzed and that adequate control of the potential hazard is implemented in the design.

As soon as sub-systems are designed in sufficient detail, or well into concept design for facilities acquisition, the SSHA can begin. Design changes to components also need to be evaluated to determine whether the safety of the system is affected. The techniques used for this analysis must be carefully selected to minimize problems in integrating sub-system hazard analyses into the System Hazard Analysis (SHA). The SSHA may be documented in a combination of text and/or tabular format.

At a minimum, there should be information for:

- The sub-system, item, or component being analyzed
- Its function
- The hazards and risks
- The severity
- The likelihood of the risk. This likelihood should be based on existing controls.
- Controls (design, safety device, warning device, procedure, and personnel equipment)
- Reduction of risk (risk severity and probability), if known
- Methods for confirming risk controls

- Recommended corrective actions should include any non-existing method for the control of the risk. Corrective changes to bring the sub-system into compliance with contractual requirements should already have been made.
- Status (open or closed)

C.2.36. System Hazard Analysis (SHA)

OVERVIEW: In acquisitions, the general purpose of the SHA is to perform a detailed safety risk assessment of a system, in particular, the interfaces of that system with other systems and the interfaces between the sub-systems that compose the system under study. The SHA should be completed after all SSHAs are complete.

The SHA is used to:

- Verify system compliance with safety requirements contained in system specifications and other applicable documents;
- Identify previously unidentified hazards associated with the sub-system interfaces and system functional faults;
- Assess the risk associated with the total system design, including software, and specifically of the sub-system interfaces; and
- Recommend actions necessary to eliminate identified hazards and/or control their associated risk to acceptable levels.

An SHA is accomplished in much the same way as the SSHA. However, as the SSHA examines how component operation or risks affect the system, the SHA determines how system operation and hazards can affect the safety of the system and its sub-systems. The SSHA, when available, serves as input to the SHA.

The SHA should include a review of sub-system interrelationships for:

- Compliance with specified safety design criteria
- Possible independent, dependent, and simultaneous hazardous events including system failures; failures of safety devices; common cause failures and events; and system interactions that could create a hazard or result in an increase in mishap risk
- Degradation in the safety of a sub-system or the total system from normal operation of another sub-system
- Design changes that affect sub-systems
- Effects of reasonable human errors
- Determination:
    - Of potential contribution of hardware and software (including that which is developed by other sources, or Commercial Off-The-Shelf hardware or software) events, faults, and occurrences (such as improper timing) on safety of the system
    - That the safety design criteria in the hardware, software, and facilities specification(s) have been satisfied
    - That the method of implementation of the hardware, software, and facilities design requirements and corrective actions has not impaired or degraded the safety of the system nor has it introduced any new hazards

The SHA should begin as the system design matures, at the preliminary design review or the facilities concept design review milestone and should be updated until the design is complete. Design changes will need to be evaluated to determine their effects on the safety of the system

and its sub-systems. This analysis should contain recommended actions, applying the Safety Order of Precedence, to eliminate or reduce the risk of identified hazards. The techniques used to perform this analysis must be carefully selected to minimize problems in integrating the SHA with other hazard analyses. The SHA may be documented in text and/or tabular format or a combination of both text and tables.

C.2.37. System-Theoretic Process Analysis (STPA)

OVERVIEW: STPA is a hazard analysis technique for complex systems developed by Nancy G. Leveson, Ph.D., of the Massachusetts Institute of Technology (MIT). STPA is based on systems theory and is a proactive evolution of the System Theoretic Accident Model and Processes (STAMP) accident causality model.

METHOD: The STPA Handbook describes the four steps of a basic STPA analysis:

> "Defining the purpose of the analysis is the first step with any analysis method. What kinds of losses will the analysis aim to prevent? Will STPA be applied only to traditional safety goals like preventing loss of human life or will it be applied more broadly to security, privacy, performance, and other system properties? What is the system to be analyzed and what is the system boundary? These and other fundamental questions are addressed during this step.
>
> The second step is to build a model of the system called a control structure. A control structure captures functional relationships and interactions by modeling the system as a set of feedback control loops. The control structure usually begins at a very abstract level and is iteratively refined to capture more detail about the system. This step does not change regardless of whether STPA is being applied to safety, security, privacy, or other properties.
>
> The third step is to analyze control actions in the control structure to examine how they could lead to the losses defined in the first step. These unsafe control actions are used to create functional requirements and constraints for the system. This step also does not change regardless of whether STPA is being applied to safety, security, privacy, or other properties.
>
> The fourth step identifies the reasons why unsafe control might occur in the system. Scenarios are created to explain:
>
> 1. How incorrect feedback, inadequate requirements, design errors, component failures, and other factors could cause unsafe control actions and ultimately lead to losses.
> 2. How safe control actions might be provided but not followed or executed properly, leading to a loss.
>
> Once scenarios are identified, they can be used to create additional requirements, identify mitigations, drive the architecture, make design recommendations and new design decisions (if STPA is used during development), evaluate/revisit existing design decisions and identify gaps (if STPA is used after the design is finished), define test cases and create test plans, develop leading indicators of risk, and for other uses as described in later chapters of [the] handbook."[32]

[32] Source: N.G. Leveson and J.P. Thomas, *STPA Handbook*, March 2018

C.2.38. Weibull Distribution

OVERVIEW: The Weibull distribution is commonly used to model event data. The main advantages of the Weibull distribution are that it can model a variety of data, it handles suspensions (non-event points) easily, and it provides a simple graphical solution and description of the data. Weibull is frequently used to model the probability of failure in aircraft components; but, as mentioned, its usefulness extends to any type of event whose probability of occurrence varies as a function of some measure of its age.

The Weibull distribution plots cumulative percent occurring as a function of time (hours, cycles, flights, years). The Weibull is defined by two parameters: the shape parameter, called the slope or beta (β), and the characteristic life, eta (η). These parameters define the specific distribution just as the mean and standard deviation define a normal distribution. Therefore, note that "-3 sigma" has no meaning against a Weibull distribution. The correct term is Bx.x life, where x.x is the percent of the distribution experiencing the event. A commonly used value for minimum life from a Weibull is the B0.1, which is the 1/1000 failure life (0.1% of the population).

A Weibull slope equal to 1 implies a random distribution; in other words, the event is unrelated to age or time. A slope greater than 1 is a wearout distribution – the event or failure is more likely the older the unit or component. The steeper the slope, the more precipitous the wearout. Physical components are typically subject to wearout failures. A slope of less than 1 is infant mortality—the failure is more likely for new or young components or units and the probability of failure diminishes with age. Mistakes in production leading to defective units may have an infant mortality problem. Errors during maintenance can likewise result in infant mortality (with the relevant time parameter being time since maintenance).

Some Weibulls require a third parameter, incubation time (t_0), for parts that are not at risk of the event until a given point in their life.

Weibulls can also be used to model events other than failures; for example, it is frequently informative to plot crack data. In this case, the Weibull represents a crack discovery distribution rather than a pure occurrence distribution. The part is inspected at some age and found to be cracked; the actual crack initiation occurred at some point prior to the inspection. Depending on the precision needed, fracture mechanics can sometimes be used to 'back up' the time of the crack to estimated initiation.

Weibulls can also be used to evaluate differences between populations (original equipment and new designs) and are able to achieve usable results even with serious deficiencies in the data.

METHOD: Cumulative percent occurring is more formally called the cumulative density function (CDF). The CDF of the Weibull distribution is:

a. $F(t) = 1 - e^{-(t/\eta)^{**}\beta}$

Where t is the given time unit; β is the slope and η is the characteristic life.

It is possible to plot a Weibull by hand on special Weibull probability paper. Positioning each event or failure point relative to the X axis is straightforward; it is simply the age of the unit in the relevant time parameter (cycles since new; hours since shop visit, etc.). Positioning the point on the Y axis (CDF) is more problematic—it involves consideration of all the *non*-failure units (suspensions) between the current failure point and the previous one. There are various algorithms for calculating this Y-position; refer to *The New Weibull Handbook*© by Dr. Robert

Abernethy or other Weibull reference material. The points are then joined by a hand-drawn best-fit line. The analyst then calculates the slope β from rise over run on Weibull paper. The characteristic life η is the time value (on the X axis) corresponding to where the line crosses 63.2% on the Y axis (CDF).

Typically, however, the analyst will use a computer software program to generate the Weibull plot with a best-fit line. The software will also allow 'what-if' evaluations using different failure distributions and criteria for modeling the distribution.

The event points should plot in a straight line, or near to it, on Weibull probability paper. If they do not, there may be multiple failure modes in the data. It is also possible there are anomalies in the data, or that a Weibull distribution is not appropriate to model the data.

The instantaneous failure probability is the probability that the part will fail in the next time unit given that it hasn't failed yet. The equation is calculated from the CDF (from formula *a.* above) for the next time unit minus the CDF in the current time unit divided by 1 minus the CDF in the current time unit:

b. [F(t+1) - F(t)] / [1 - F(t)]

Where F( ) is the percent occurring (CDF) as calculated by formula *a.* above. One cannot simply take the difference between F(t+1) and F(t); the fact the unit has not failed at its current age (t) *must* be taken into account.

This formula can also be used to calculate the probability of failure (or other event) in any time interval *x* by replacing (t+1) in formula *b.* with (t+x).

Weibulls are often performed with few failures; in fact, Weibulls can be performed without any failures or other events by assuming a slope (informed by experience) and assuming that one failure or event has occurred. This provides a picture of how good the experience has proven so far. This type of Weibull is called a Weibayes. Weibayes can also be performed when there are multiple failures; the difference between a Weibull and a Weibayes is that the Weibull plots the best fit through the actual failure data, whereas the Weibayes plots what the distribution *should* look like given the number of failures and the times on all the units (simplistically, it picks the most likely failures rather than the actual failures). Comparisons between the Weibull and the Weibayes for the same data provide understanding into the underlying population. If the two lines are close together, the population is homogenous. If the lines are far apart, there are likely multiple populations in the data, or only a sub-population is at risk of the event. Confidence intervals are used to provide statistical evaluation of the closeness of the lines.

Once the analyst has a Weibull plot with its associated parameters, this distribution can be used to calculate future risk of events, whether visually (via graphical use of formula *b.*—remember *not* to simply subtract the current point from the future point), through calculation, or as input to a Monte Carlo Simulation.

RELATIONSHIP TO OTHER STATISTICAL DISTRIBUTIONS: Log-normal distributions are also used to model failure data. A log-normal distribution converts failure data to a normal distribution by taking the log of each point and plotting the transformed data. No particular distribution is inherently better than the other; it is simply a question of which best fits the data. Often, adequate results can be achieved with several different distributions, especially those in the same general family (such as Weibulls, log-normals, and exponentials). Note that a Weibull collapses to an exponential distribution when the Weibull slope is equal to 1, which is indicative

of a random failure mode. An un-transformed normal distribution is usually not a good descriptor of failure data. Normal data is evenly distributed about the average value, whereas failure data tends to extend much higher above the average value than it does below. A Weibull can be used to model normally distributed data; the Weibull slope of normally-distributed data is 3.44.

RESOURCES: Various commercially available software programs exist. The FAA's Aircraft Certification has a site license for SuperSmith™ by Fulton Findings, LLC. Microsoft Excel™ also has some functionality.

EXAMPLE: The following graph is an example of a software-generated Weibull distribution for a population with 6 failures out of 22 units. Note that the 'dogleg' (apparent slope change) in the failure points might be an indicator of multiple failure modes.

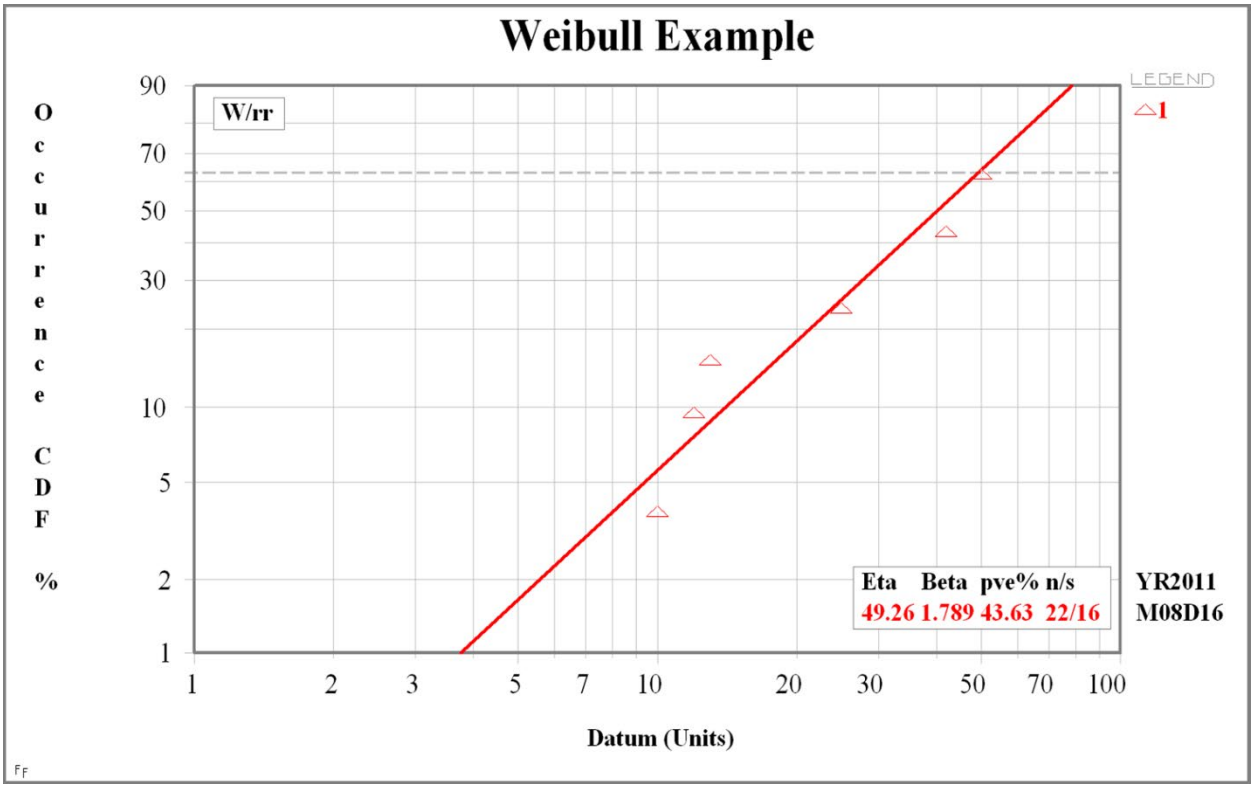


Figure C-26: Weibull Example

C.2.39. "What If" Tool

PURPOSE: The "What If" tool is one of the most powerful hazard identification tools. As in the case of the Scenario Process tool, 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. 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 (OA) 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 to determine what could go wrong. 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.
- Don't dwell on grammatical details.
- Include elements of Mission, (hu)Man, Machine, Management, and Media.
- Start with history.
- Encourage imagination and intuition.
- Carry the scenario to the worst credible outcome.
- Use a single person or group to edit.

RESOURCES: A key resource for the "What If" tool is the Operations Analysis. It may be desirable to add detail to it in the area to be targeted by the "What If" analysis. However, in most cases an OA can be used as-is, if it is available. The "What If" tool is specifically designed to be used by personnel actually involved in an operation. Therefore, the most critical "What If" resource is the involvement of operators and their first lines supervisors. Because of its effectiveness, dynamic character, and ease of application, these personnel are generally quite willing to support the "What If" process.

COMMENTS: The "What If" tool is so effective that the Occupational Safety and Health Administration (OSHA) has designated as it one of six tools from among which activities facing

catastrophic risk situations must choose under the mandatory hazard analysis provisions of the process safety standard.

EXAMPLES: The following is an extract from the typical output from the "What If" tool.

Example "What If" Analysis

Situation: Picture a group of three 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 for example 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 steps of the SRM process.

C.3. Assess Safety Risk Tools

C.3.1. Risk Matrix

A risk matrix is a graphical means of determining safety risk levels. The columns in the matrix reflect severity categories; its rows reflect likelihood categories. The 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.

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.

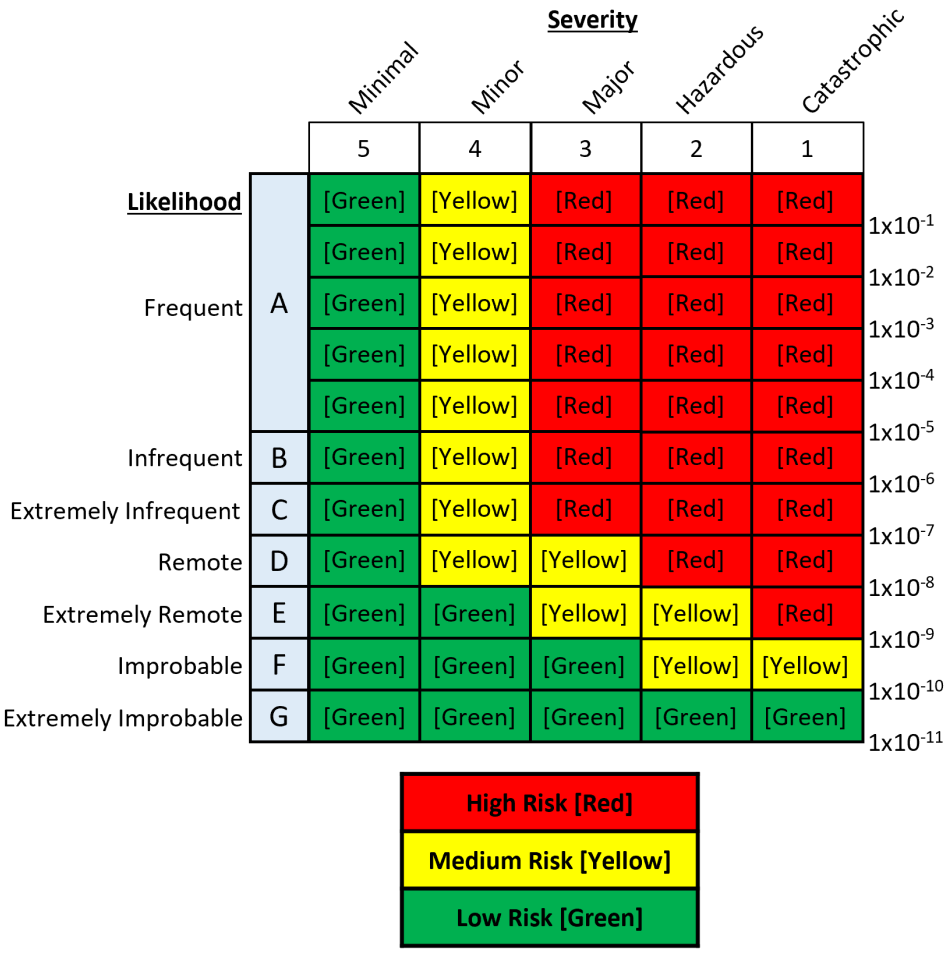


Figure C-27: Risk Matrix for Commercial Aviation

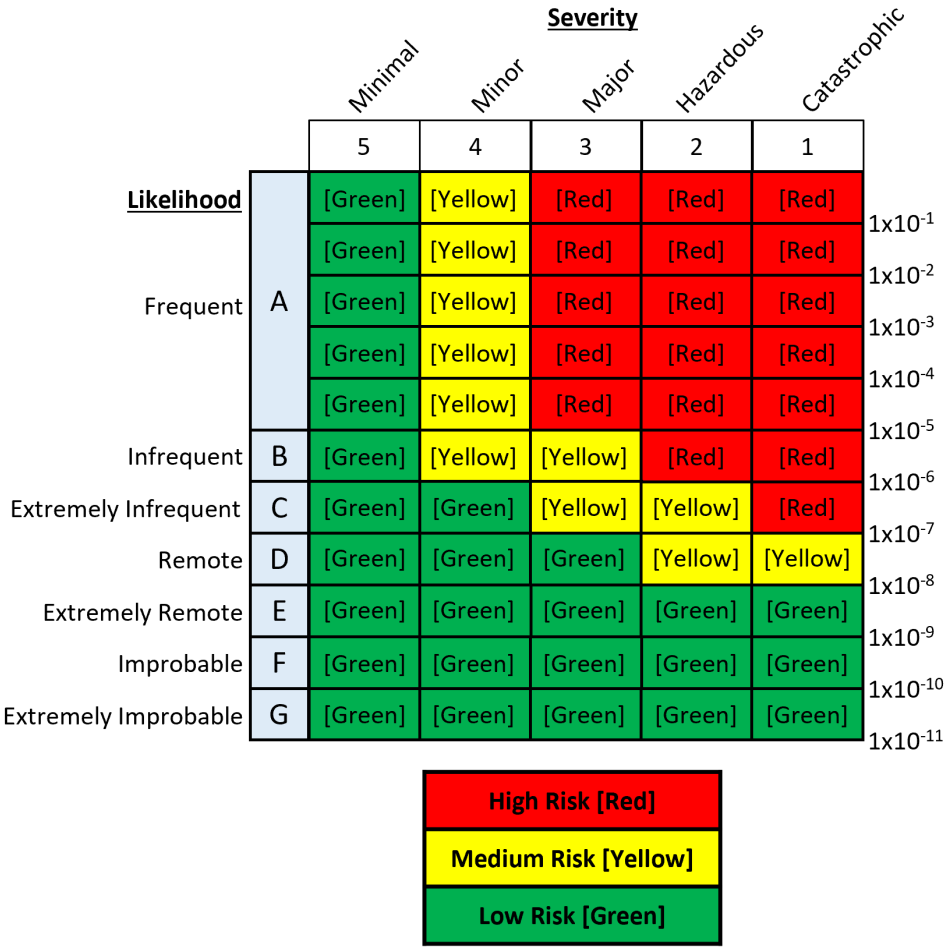


Figure C-28: Risk Matrix for General Aviation

Using the risk matrix, each hazard is ranked and prioritized according to its associated safety risk levels following the steps below:

- When appropriate, rank hazards according to their associated safety risk levels (illustrated by where they fall on the risk matrix).
- Plot the severity and likelihood of the effect associated with the hazard using the logarithmic scale.
- If any of the plotted points fall within the red region, the safety risk associated with the hazard is high; if any of the plotted points fall within the yellow region with none in the red, the safety risk associated with the hazard is medium; otherwise, the risk is low.
- Once mitigations are developed and the analysis is conducted, taking into account those mitigations, the residual safety risk is plotted. Plotting the prediction of the residual risk illustrates the impact of the safety risk controls on the initial safety risk and shows the decision maker whether the safety risk associated with the hazard will be mitigated to an acceptable level.

C.4. Control Safety Risk Tools

C.4.1. Safety Order of Precedence

The following table shows the Safety Order of Precedence. Safety professionals use the techniques listed, in priority order, for reducing risk.

Table C-4: Safety Order of Precedence

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

The following are examples of the Safety Order of Precedence.

Description	Example
Design for Minimum Risk:	Design hardware systems in accordance with FAA-G-2100g, i.e., use low voltage rather than high voltage where access is provided for maintenance activities.
Incorporate Safety Devices	If low voltage is unsuitable, provide interlocks.
Provide warning devices	If safety devices are not practical, provide warning placards.
Develop procedures and training	Train maintainers to shut off power before opening high voltage panels.

Appendix D. SRM Technical Definitions

Data-driven decision making requires tools beyond judgmental methods to support Safety Risk Management (SRM). For example, quantitative techniques (machine learning, statistics, reliability engineering, etc.) enable analysts to estimate the degree to which hazards contribute to risk, facilitating the prioritization of mitigations. This appendix provides quantitative interpretations of key terms, while also providing more context for data scientists and statisticians.

D.1. Expected Value

Definition: The expected value of a random variable, X, is the weighted average of possible values that X can take, where each value, x, is weighted by the associated probability, $P\{X = x\}$. Expected value is also referred to as *expectation* or *mean*. The expected value of X is written as $E[X]$. In the case of discrete random variables:

$$E[X] = \sum_{x} xP\{X = x\}$$

In the case of continuous random variables (where $f(x)$ is the probability density function):

$$E[X] = \int_{-\infty}^{\infty} xf(x)dx$$

Example: The probability of an accident on an individual flight is p; the number of flights (exposure) is n. The number of accidents, X, in n flights is a binomial random variable. The expected number of accidents is the individual per-flight probability of an accident times exposure: $E[X] = np$. For example, if the per-flight probability of an accident is 0.000001 and the exposure is 1,000,000 flights, the expected number of accidents in 1,000,000 flights is 1 ($10^{-6} \times 10^{6}$).

D.2. Hazard

Discussion: The term *hazard* has a long, varied, and sometimes contentious history. In the simplest terms, “hazard” is a common English word; Merriam-Webster, for example, defines it as “a source of danger,” which immediately leads to the definition of “danger” (“exposure or liability to injury, pain, harm, or loss”), which can be combined to “Hazard: a source of exposure to loss.” Within the aviation environment, loss can be defined as “undesired states or outcomes.” Some organizations may choose to extend the “undesired states or outcomes” to operational areas; others may focus solely on threats to human life. Nonetheless, the verbal rendering communicates a basic understanding.

“Hazard” has also been more specifically defined in Federal Aviation Regulations:

> Title 14 of the Code of Federal Regulations (CFR) part 5 Hazard: A condition or an object that could foreseeably cause or contribute to an incident or aircraft accident, as defined in 49 CFR 830.2.

> 49 CFR § 830.2 Aircraft accident: An occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight and all such persons have disembarked, and in which any person suffers death or serious injury, or in which the aircraft receives substantial damage. For the purposes of this part, the definition of "aircraft accident" includes "unmanned aircraft accident," as defined herein.

Hazard has also been defined in Federal Aviation Administration (FAA) Orders and policy documents for the purpose of guidance. For example, the Air Traffic Organization (ATO) Safety Management System (SMS) Manual defines it as: "Any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. A hazard is a prerequisite to an accident or incident."

A mathematical definition of "hazard" is also possible. This symbolic definition serves to establish a quantifiable relationship to the undesired states and provides guidance relative to quantitative models (e.g., fault trees, event trees, Bayesian networks, causal inference models).

Definition: A hazard is defined as a condition or an object with the potential to cause or contribute to an incident or aircraft accident, as defined in 49 CFR § 830.2. Mathematically, a hazard is a condition that would increase the probability of an aircraft accident or incident. Let A_i equal a type i aircraft accident, and let X_j equal a given condition, j. X_j is a hazard with respect to A_i, if the probability of an aircraft accident or incident, conditional on X_j, is greater than the unconditional probability of A_i. In symbols, X_j is a hazard if:

$$P(A_i \mid X_j) > P(A_i)$$

In other words, if the overall probability (considering all causes and contributing factors) of a Loss of Control (LOC) accident is 1×10^{-7}, but the specific probability of LOC given incorrect flap setting probability is 1×10^{-6}, incorrect flap setting is a hazard for LOCs.

This definition supports quantitative analyses of potential hazards but is not intended to supplant subject matter expertise. For example, if $P(A_i \mid X_j)$ exceeds $P(A_i)$ by an extremely small amount, then decision-makers may conclude that X_j is not, for practical purposes, a hazard. The degree to which $P(A_i \mid X_j)$ must exceed $P(A_i)$ in order to require mitigation is highly dependent on context. Thus, this definition does not set numerical limits, but simply recognizes that expert judgment is a critical input in the hazard analysis process.

Examples: The symbolic representation facilitates data-driven hazard analyses in two contexts: (a) a deterministic framework where the relationships between hazards and outcomes are regarded as fully known, and (b) a statistical framework where there is uncertainty (e.g., where information about the candidate hazard is obtained through sampling). The following examples illustrate applications of this probabilistic definition.

Deterministic framework example: Fault Tree Analysis.

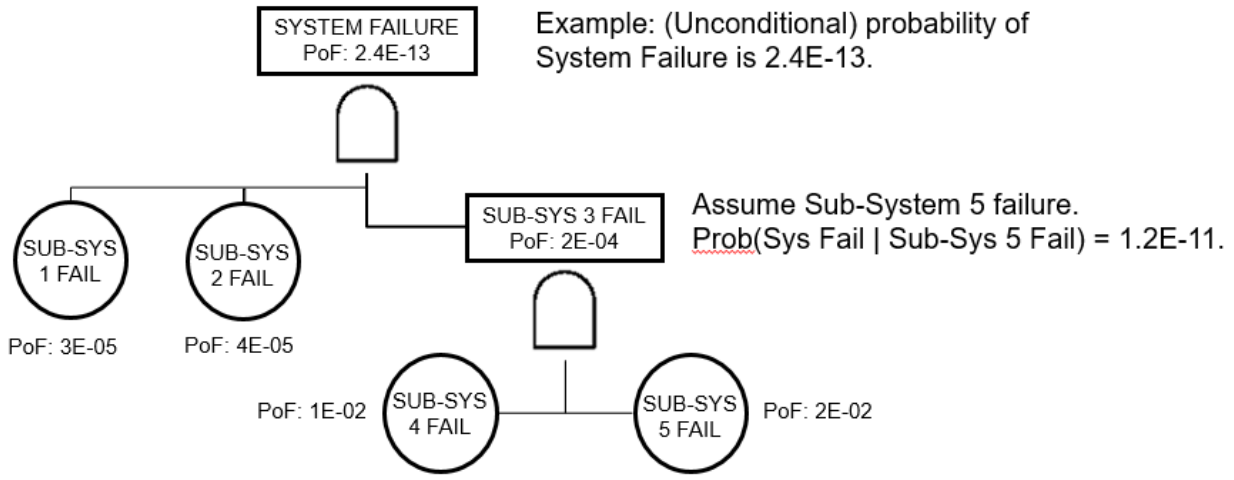


Figure D-1: Fault Tree Analysis

In the example, the paths through which hazards lead to the top event (in this case an aircraft system failure), and associated probabilities, are fully known. System failure results from the combined failures of sub-systems 1, 2 and 3. Sub-system 3 failure, in turn, depends on the failure of sub-systems 4 and 5. In this example, all sub-systems must fail in order for the system to fail. The probability of failure (PoF) for the entire system is the product of the failure probabilities for sub-systems 1-3:

Prob(System Failure) = $(3 \times 10^{-5}) \times (4 \times 10^{-5}) \times [(1 \times 10^{-2}) \times (2 \times 10^{-2})] = (2.4 \times 10^{-13})$

However, the system failure probability, given that sub-system 5 has failed is:

Prob(Sys. Fail | Sub-sys. 5 fail) = $(3.0 \times 10^{-5}) \times (4 \times 10^{-5}) \times [(1 \times 10^{-2}) \times 1] = (1.2 \times 10^{-11})$

Thus, sub-system 5 failure is a hazard. More generally, fault trees give an explicit estimate of the contribution of each sub-system to total system failure probability. An advantage of this framework is that failure modes are fully represented in the model. The disadvantage is that there may be unknown failure modes (e.g., unidentified “sneak circuits”), and so the model may underestimate true system risk.

Statistical framework example: simple comparison between two proportions.

Fault trees are useful in applications where it is possible to describe schematically the interaction between system components. In other applications, a deterministic system model is not possible, and a statistical model may be required. However, because a statistical model is based on a sample of data, the answer to the question “is ‘X’ a hazard?” is probabilistic.

The following data represents operations and accident counts for a 12-year period for towered and non-towered airports. For airports as a whole, the estimated per-operation probability of an accident is $P(A_i) = (10.17 \times 10^{-6})$. The estimated accident probability, given the no-tower condition, is $P(A_i \mid X_j) = (12.33 \times 10^{-6})$.

Table D-1: Operations, Accident Counts, and Accident Rates for Towered (Class D) and Non-Towered Airports

Airport Type	Operations (mil)	Accidents	Rate (per million)
Tower	397.69	2,760	6.94
No Tower	595.04	7,337	12.33
Total	992.73	10,097	10.17

Estimated $P(A_i \mid X_j)$ is greater than estimated $P(A_i)$, but random chance could have produced this result, even though there is no difference in the true accident probabilities. A statistical test is applied to determine if the observed difference is "significant" in the sense that it is unlikely to have been produced by chance. The test is a function of: (1) sample sizes (large samples would give more confidence that the observed difference is not random) and; (2) the size of the difference between the two rates (a large difference would be evidence that the difference is not random).

$$Z = \frac{(p_2 - p_1)}{\sqrt{\hat{p}(1-\hat{p})\left(\frac{1}{n_2} + \frac{1}{n_1}\right)}}$$

Where Z is a measure of the relative significance of the difference between p_1 and p_2 given the underlying variability of each population.

In this example, the value of Z is approximately 12, so that the probability that the observed difference is a random fluke and that there is no true underlying difference, is effectively zero.

Statistical framework example: multivariate case.

While direct comparison between estimated rates may be sufficient evidence that a given condition is a hazard in many cases, there are circumstances where this is not true. In the previous example, a statistically significant difference is observed between towered and non-towered airports. However, it is possible that this difference reflects the fact that better pilots tend to operate at towered airports and that the underlying hazard is "inferior pilot quality" rather than a lack of Air Traffic Control Tower (ATCT) services.

More generally, an investigation into whether one factor, X_j, is a hazard sometimes may require controlling for other covariates. In symbols, the resulting model would have the form:

$$E(A_i \mid X_j, C)$$

Where $E(.)$ is the expected value, A_i is accident type i, X_j is condition j, and C is a vector of control variables. Again, whether X_j is a hazard is an empirical question, and not determined *a priori* by expert judgment; it is a purely data-driven approach. In some contexts, this is referred to as conditional structural expectation.

A concrete example of such a model is the Poisson regression. Let A_i be a random variable that represents the number of accidents of type i. The number of accidents is conditioned on factors x. Then in the Poisson regression, the probability that Ai will be equal to a specific value, a, conditional on x, is:

$$P(A_i = a|\boldsymbol{x}) = \frac{e^{-\mu_i}\mu_i^a}{a!}, \quad a = 0,1,2,\ldots$$

Thus, the Poisson function returns the probability of event(s) given the expected number of events. Tables of the Poisson function are readily available online, in Excel, or in statistics handbooks.

Where the expected value is a log-linear model (with parameter β):

$$E[a|\boldsymbol{x}] = \mu_i = exp(\beta \boldsymbol{x})$$

This model provides a way to measure the effect of condition *x* on the expected number of accidents. If an increase in *x* (or the presence of *x* in the case of a binary variable) increases the number of accidents, and the effect is statistically significant, then this would be empirical evidence that *x* is a hazard.

D.3. Probability

Definition: An expression of uncertainty that quantifies the extent to which something happening. Formally, define the sample space, *S*, as the set of all possible outcomes of a random experiment whose outcome is not predictable with certainty. An event, *E*, a subset of *S*, is a set of possible outcomes that satisfy a given property. Probability may then be defined as a function, *P*, that maps events, *E*, to the set of real numbers, and satisfies the following three properties:

1. Probability is greater than or equal to 0, and less than or equal to 1. $0 \leq P(E) \leq 1$ for every allowable event, *E*. In other words, all probability values fall within the values of zero and one, inclusively.
2. The certain event, the event that some outcome occurs, has a probability of 1. $P(S) = 1$. That is, for any possible outcomes that are mutually exclusive, the probability that one or the other occurs is the sum of the individual probabilities.
3. The probability of the union of *mutually exclusive* events, E_1, E_2, …, is the sum of the probabilities of the individual events. In other words, when the probability of all possible events is added together, the sum must equal 1. In symbols:

$$P\left(\bigcup_{i=1}^{\infty} E_i\right) = \sum_{i=1}^{\infty} P(E_i)$$

Where $E_iE_j = \varnothing$, when $i \neq j$.

The numeric value may also be assigned subjectively, representing a degree of belief or judgment. In cases where the number of occurrences is small relative to the measure of exposure, the numeric value can be estimated by the relative frequency of an occurrence; for example, the number of accidents divided by the total number of flights. (For a discussion of the relationship between rates and probabilities, see *Rate* definition.)

Examples:

1. A subject matter expert (SME) believes that the per-flight probability of a pilot error during the approach phase of flight is 1/100 or 0.01.

2. The estimated per-flight probability of an accident involving a specific type of general aviation aircraft, based on a sample that had 10 events in 1,000,000 general aviation flights, giving 10 ÷ 1,000,000; or 0.000001.
3. An analyst observes that the rate of pilot deviations in a given sector is 1 per 1,000 operations, or 0.001 per operation. Under the assumption that the number of pilot deviations is Poisson distributed, she computes the probability of a pilot deviation (at least one) in 1,000 operations as 0.632.

D.4. Rate

Definition: The frequency of an occurrence, expressed as the ratio of the number of occurrences relative to a measure of exposure such as operations, cycles, flight hours, departures, or launches.

Example: The number of in-flight shutdowns (IFSDs) is 10,000 in one million flight hours; or 10,000 ÷ 1,000,000 = 0.01 per flight hour.

The Relationship Between Rate and Probability: The rate-to-probability conversion depends on specific assumptions regarding the process that generates the phenomenon under study. For small values, the rate approximates individual probability. For example, if the IFSD rate is 0.01 per flight hour, then under the assumption that IFSD are Poisson distributed, the probability of an IFSD during one flight hour is 0.00995 ≈ 0.01. However, if the IFSD rate is 0.5 per flight hour, then the probability of an IFSD during one flight hour is 0.3935. If the IFSD rate is 10 per flight hour, then the probability of an IFSD during one flight hour is 0.99995. In general, the approximation is acceptable at a 0.03 rate or below as the Poisson function returns.

Example: Let X equal the number of inflight shutdowns in 10 flight hours. The rate of inflight shutdowns per flight hour is $r = 0.01$; and so the rate for 10 flight hours is $\lambda = 10r = 0.1$. The probability of x inflight shutdowns is:

$$P(X = x) = \frac{(e^{-\lambda})(\lambda)^x}{x!}$$

The probability of no inflight shutdowns, $x = 0$, in 10 flight hours is:

$$P(X = 0) = \frac{(e^{-0.1})(0.1)^0}{0!} = e^{-0.1} = 0.9048 = 90.48\%$$

The probability of one inflight shutdown, $x = 1$, in 10 flight hours is:

$$P(X = 1) = \frac{(e^{-0.1})(0.1)^1}{1!} = 0.1e^{-0.1} = 0.0905 = 9.05\%$$

The probability of an inflight shutdown, $x \geq 1$, in 10 flight hours is:

$$P(X \geq 0) = 1 - P(X = 0) = 1 - 0.9048 = 0.0952 = 9.52\%$$

D.5. Risk

Definition: A generic expression that describes the probability of an outcome of a given severity. In practice, risk is specific to an affected population, exposure, and a given hazard (individual risk, individual personal risk, collective risk, etc.). Risk can be expressed in terms of

rates or probabilities. With respect to FAA Order 8040.4, losses are classified using severity categories (see Table C-1, Severity Definitions, within the order).

Examples:

1. Risk expressed in terms of rate: Three hazardous events per 10 years.
2. Risk expressed in terms of probability: The per-flight probability of a catastrophic outcome is 6×10^{-9}; the per-flight probability of a hazardous event is 5×10^{-6}.

In the figure below, risk, $P(ls)$, is the per-flight probability of a loss of severity s. The acceptability of $P(ls)$ is determined by its placement in the risk matrix.

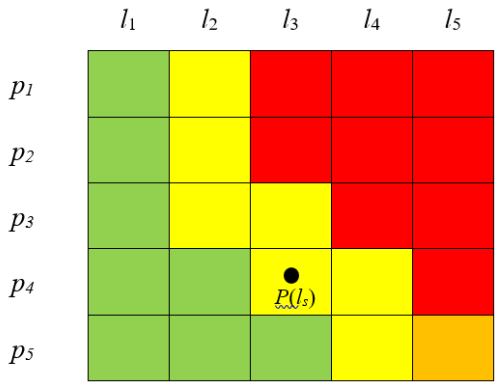


Figure D-2: Risk Plotted on a Matrix

D.6. Individual Risk

Definition: The probability of a given outcome per unit of exposure (per operation, flight hour, opportunity, etc.) as a result of a given hazard.

Examples:

1. The probability that an individual flight will experience a fatal accident due to an inflight fire.
2. The probability of an IFSD per flight hour.
3. The probability of an aborted takeoff per departure.

D.7. Individual Personal Risk

Definition: The probability that any single person will experience a given outcome per flight.

Examples:

1. Passenger Example. The probability that a passenger suffers a fatal injury during a flight.
2. Flight Attendant Example. The probability that a flight attendant suffers an injury during a turbulence event.

Appendix E. Acronyms

AC - Advisory Circular

AGC - Office of the Chief Counsel

AIDS – Accident and Incident Data System

AMASS - Airport Movement Area Safety System

AMOC - Alternative Methods of Compliance

ANG - Next Generation Air Transportation System

ARP - Airports

ARTCC - Air Route Traffic Control Center

ASDE-X - Airport Surface Detection System — Model X

ASH - Security and Hazardous Materials Safety

ASIAS - Aviation Safety Information Analysis and Sharing

ASL - Aerospace System Level

ASOR - Allocation of Safety Objectives and Requirements

AST - Commercial Space Transportation

ATC - Air Traffic Control

ATCT - Air Traffic Control Tower

ATM - Air Traffic Management

ATO - Air Traffic Organization

ATS - Air Traffic Services

ATSI - Air Traffic Safety Inspector

AVP - Accident Investigation and Prevention

AVP-300 - Safety Management Division

AVP-310 - Safety Risk Management and Safety Assurance Branch

AVP-320 - Safety Policy and Promotion Branch

AVS - Aviation Safety

AVS-1 - Associate Administrator for Aviation Safety

AVSSMS - Aviation Safety Safety Management System

CA - Conflict Alert

CCFA - Common Cause Failure Analysis

CDF - Cumulative Density Function

CENRAP - Center RADAR Processing

CFR - Code of Federal Regulations

CNS - Communication, Navigation, and Surveillance

CONOPS - Concept of Operations

CSA - Comparative Safety Assessment

DARC - Direct Access Radar Channel

DOT - Department of Transportation

EFAS - En Route Flight Advisory Service

EOR - Electronic Occurrence Reports

ETA – Energy Trace Analysis

ETBA - Energy Trace and Barrier Analysis

FAA - Federal Aviation Administration

FCAA - Foreign Civil Aviation Authority

GA - General Aviation

GAO - Government Accountability Office

GPWS - Ground Proximity Warning System

HAW - Hazard Analysis Worksheet

HAZOP - Hazard and Operability Tool

HEA - Human Error Analysis

HEAT - Hazard Enterprise Assessment Tool

HIRMT - Hazard Identification, Risk Management & Tracking

IFR - Instrument Flight Rules

IFSD - In-flight Shutdown

IMC - Instrument Meteorological Conditions

JHA - Job Hazard Analysis

JRC - Joint Resources Council

JTA - Job Task Analysis

KSN - Knowledge Sharing Network

LOB - Line of Business

LOC - Loss of Control

M - Million

MBSE - Model-Based System Engineering

MES - Multi-Linear Events Sequencing

MIT - Massachusetts Institute of Technology

MOR - Mandatory Occurrence Report

MORT - Management Oversight and Risk Tree

MPM - Mitigation Performance Monitoring

MSAW - Minimum Safe Altitude Warning

NAS - National Airspace System

NCP - NAS Change Proposal

NTSB - National Transportation Safety Board

O&SHA - Operating and Support Hazard Analysis

OA - Operations Analysis

OED - Operational Environment Description

OHA - Operational Hazard Assessment

OIG - Office of Inspector General

OMB - Office of Management and Budget

OPR - Office of Primary Responsibility

ORM - Operational Risk Management tool

OSA - Operational Safety Assessment

OSED - Operational Services and Environment Description

OSHA - Occupational Safety and Health Administration

PHA - Preliminary Hazard Analysis

PHL - Preliminary Hazard List

POC - Point of Contact

PoF - Probability of Failure

R&D - Research and Development

RCA - Root Cause Analysis

SCMP - Strategic Compliance Monitoring Plan

SCT - Safety Collaboration Team

SEC - System Engineering Council

SHA - System Hazard Analysis

SMC - Safety Management Council

SME - Subject Matter Expert

SMS - Safety Management System

SOP – Standard Operating Procedure

SRM - Safety Risk Management

SRMGSA - Safety Risk Management Guidance for System Acquisitions

SSHA - Subsystem Hazard Analysis

SSP - State Safety Program

STAMP - System Theoretic Accident Model and Processes

STEP - Sequential Time Event Plot

STPA - System-Theoretic Process Analysis

TCAS - Traffic Alert and Collision Avoidance System

TRACON - Terminal Radar Approach Control Facility

UAS - Unmanned Aircraft Systems

U.S. - United States

VFR - Visual Flight Rules

VMC - Visual Meteorological Conditions

Appendix F. Related Documents

F.1. Code of Federal Regulations (CFR)

Title 14 CFR parts 5, 121, 135, 145, 61, 63, 65, 67, 91, 120, and 183

Title 49 CFR part 40

F.2. FAA Orders

8000.369, *Safety Management System*

8040.4, *Safety Risk Management Policy*

JO 1000.37, *Air Traffic Organization Safety Management System*

5200.11, *FAA Airports (ARP) Safety Management System*

8200.1, *United States Standard Flight Inspection Manual*

1800.66, *Configuration Management Policy*

VS 8000.367, *Aviation Safety Safety Management System (AVSSMS) Requirements*

1100.161, *Air Traffic Safety Oversight*

8110.107, *Monitor Safety/Analyze Data*

8110.100, *Special Airworthiness Information Bulletin*

8110.103, *Alternative Methods of Compliance (AMOC)*

8000.51, *Aircraft Certification Service Delegation of Authority*

4040.26, *Aircraft Certification Service Flight Test Risk Management Program*

JO 7110.65, *Air Traffic Control*

6000.15, *General Maintenance Handbook for National Airspace System (NAS) Facilities*

JO 3000.57, *Air Traffic Organization Technical Operations Training and Personnel Certification*

JO 8240.3, *Certification of Flight Inspection Personnel*

8000.368, *Flight Standards Service Oversight*

8900.1, *Flight Standards Information Management System*

AM 1110.155, *Aerospace Medicine Safety Management Council (SMC)*

9120.1, *Drug and Alcohol Compliance and Enforcement Inspector Handbook*

8040.6, *Unmanned Aircraft Systems (UAS) Safety Risk Management (SRM) Policy*

5300.1, *Modifications to Agency Airport Design, Construction, and Equipment Standards*

8000.373, *Federal Aviation Administration Compliance Program*

NG 1000.44, *NextGen Safety Management System*

SH 8000.98, *Security and Hazardous Materials Safety (ASH) Safety Management System*

9550.8, *Human Factors Policy*

F.3. Guidance and Other Documents

ATO SMS Manual

Safety Risk Management Guidance for System Acquisitions (SRMGSA)

National Airspace System Configuration Control Board Charter

FAA-IR-M-8040.1C, Airworthiness Directive Manual

IR 8100.16, Aircraft Certification Service Policy Statement, Policy Memorandum, and Deviation Memorandum Systems

Drug Abatement Division's Strategic Compliance Monitoring Plan (SCMP)

FAA Integrated Oversight Philosophy

ARM-002-001, Rulemaking Process

AVS-002-009, Exemption Process

AVS-01-006, AVS Internal Audit Process

Advisory Circular (AC) 150/5370-2, Operational Safety on Airports During Construction

AC 150/5370-10, Standards for Specifying Construction of Airports

AST Safety Management System Manual