U.S. Department of Transportation

Federal Aviation Administration

Air Traffic Organization, Office of Safety

Safety Risk Management Guidance for System Acquisitions (SRMGSA)

Federal Aviation Administration Safety Management System (SMS) and Acquisition Management System (AMS) Guidance Document

SRMGSA FINAL
December 2008
Version 1.5

Preface

This version of the Safety Risk Management Guidance for System Acquisitions (SRMGSA) cancels SRMGSA Version 1.4a. It also supersedes the System Safety Management Program (SSMP), Revision 10 and applies to proposed system acquisition and legacy system changes to the National Airspace System upon approval. System acquisitions that were initiated under SSMP Revision 10 may continue to use that document.

Table of Contents

1.0 INTRODUCTION

This document defines the scope, purpose, objectives, and planned activities of the Federal Aviation Administration's (FAA's) system safety effort as it applies to Safety Risk Management (SRM) for all system acquisitions that provide Air Traffic Control (ATC) and navigation services in the National Airspace System (NAS).

The Safety Risk Management Guidance for System Acquisitions (SRMGSA) contributes to, and embodies, the spirit of the FAA's safety culture, which is founded on the dedication and accountability of individuals engaged in any activity that affects the safe provision of ATC services. A safety culture is a pervasive emphasis on safety that promotes an inherently questioning attitude, resistance to complacency, a commitment to excellence, and the fostering of personal accountability and corporate self-regulation in safety matters.

1.1 Purpose

The purpose of this document is to meet the requirements and implement the policy in Section 4.12 of the Acquisition Management System (AMS). Hence, this SRMGSA provides the guidance to be used by the Air Traffic Organization (ATO) in conduct of SRM.

The SRMGSA defines the FAA's plan for ensuring that system safety[1] is effectively integrated into system changes and NAS modernization in accordance with FAA orders, the Safety Management System (SMS) Manual, and AMS policy. It describes the AMS phases, organizational roles and responsibilities, program requirements, tasks, and reporting requirements associated with performing SRM within the ATO and other organizations involved in acquisitions (e.g., Office of Aviation Safety (AVS), Office of Airports). The purpose of SRM is to maintain or improve the safety of the NAS by identifying, managing, and mitigating the safety risk associated with making changes to the NAS. This SRMGSA serves as:

- SMS guidance for acquisitions during Mission Analysis (MA) and Investment Analysis (IA).
- Specific guidance for system changes.
- A definition of Joint Resources Council (JRC) expectations regarding SRM.
- General SMS guidance for Service Team planning during the Solution Implementation (SI) and In-Service Management (ISM) phases.

The SRMGSA, in conjuction with the Program Safety Plans (PSPs) of the individual Service Teams, provides a framework to ensure the execution of SRM throughout the entire lifecycle of a system or product. They also establish a disciplined methodology based on system engineering to achieve the SRM objectives, as

---

[1]The term *system* includes any product, service, and/or activity developed, produced, or managed by a specific person, agency, or organization for a designated purpose. The term *safety* includes any technical, social, educational, and/or managerial action initiated to eliminate or reduce the hazards (i.e., risk of property loss and personal injury) associated with a procedure or system.

defined in FAA orders, ATO Order JO 1000.37: Air Traffic Organization Safety Management System, the SMS Manual, and AMS policy.

This document describes the organization and responsibilities of FAA management and Service Teams for fulfilling SRM objectives. Service Team SRM is a responsibility of the Service Units (e.g., NextGen and Operations Planning Services, En Route and Oceanic Services, Terminal Services, System Operations Services, Technical Operations Services). The SRMGSA addresses the Office of Safety's relationship with the Service Units for approving safety documentation and accepting risk prior to JRC decisions.

Upon agreement among the Office of Safety, the applicable Operational Service Units (OSUs), the ATO System Safety Working Group (SSWG), and the Acquisition Systems Advisory Group (ASAG), the SRMGSA may be revised when a change affects the accepted scope of performance or requirements. The SRM Office is responsible for revising and maintaining the SRMGSA.

1.2   Scope

FAA policy (AMS policy, section 4.12), orders (e.g., FAA Order 8040.4, Safety Risk Management; FAA Order 1100.161, Aviation Safety Oversight; ATO Order JO 1000.37, Air Traffic Organization Safety Management System), and the SMS Manual mandate a planned and organized SRM approach to decision-making consistent with the role of each organization or Line of Business (LOB) in the FAA. This SRMGSA further defines the ATO SRM process. The ATO provides leadership, direction, and guidance relating to FAA acquisition policy, research, system prototype development, and agency information resource management. The ATO leads the agency's programs in the areas of:

- Definition and validation of requirements and planning for current and future systems supporting the NAS, including Air Traffic Management (ATM), airport technology, safety, capacity, and security.

- Identification of complex initiatives for new management approaches, administrative techniques, and information technology solutions to improve resource allocation, cost efficiency, and productivity.

- Integration of operational requirements with system development, including system planning for design and material control, advanced technologies and concepts, and operations research.

- Development and management of centralized acquisition policy.

1.3   List of Associated Documents

1.3.1   Government Documents

1.3.1.1   FAA Documents

1.   FAA Order 8040.4, Safety Risk Management
2.   FAA Order 1100.161, Air Traffic Safety Oversight
3.   FAA AMS
4.   ATO SMS Manual
5.   ATO Order JO 1000.37, ATO Safety Management System
6.   FAA Order 1800.66, Configuration Management Policy

1.3.2   Non-Government Documents[2]

1.   Radio Technical Commission for Aeronautics (RTCA)/DO-264 – Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications

2.   Society of Automotive Engineers (SAE) Aerospace Recommended Practice ARP4761 – Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

3.   RTCA/DO-178B – Software Considerations in Airborne System and Equipment Certification

4.   RTCA/DO-278 – Guidelines for Communication, Navigation and Surveillance/Air Traffic Management (CNS/ATM) System Software Integrity Assurance

---

[2] Use the latest version of these documents. They are not under FAA Configuration Management control.

2.0 FAA SRM POLICY

This section describes the SRM policies and guidance used within the ATO. The overarching documents are FAA Order 1100.161, Aviation Safety Oversight; ATO Order JO 1000.37, Air Traffic Organization Safety Management System; FAA Order 8040.4, Safety Risk Management; the SMS Manual; and the AMS.

2.1   SRM

FAA Order 1100.161 requires that ATO decisions in acquiring or implementing new systems be made in accordance with the ATO SMS Manual, the AMS, and the Configuration Control Change Board policies and procedures. The SMS Manual provides additional guidance for conducting SRM for changes to the NAS that may impact safety (e.g., the change impacts the issuance of safety alerts or safe separation of aircraft from each other, terrain, objects, Special Use Airspace, hazardous weather). Each Service Team and LOB is required to establish and implement the policy in the SMS Manual and FAA Order 1100.161 consistent with that Service Team's or LOB's role in the FAA. With ATO Office of Safety coordination and concurrence, the safety analysis documentation required for JRC decisions can be tailored by the FAA Acquisition Executive, Service Units Vice President, or LOB Executive with sufficient rationale. However, each Service Team and LOB must satisfy the following criteria:

Implement – SRM must be implemented by performing risk assessment and analysis and using the results to make decisions.

Plan – The risk assessment and analysis must be predetermined and documented in a plan that includes the criteria for acceptable risk.

Hazard Identification – The hazard analyses and assessments included in the plan must identify the safety risks associated with the system or operations being evaluated.

Hazard Classification through Analysis – The risks must be characterized in terms of severity of consequence and likelihood of occurrence.

Risk Assessment – The risk assessment of the hazards examined must be compared to the acceptability criteria specified in the plan and the results provided in a manner and method easily adapted for decision-making.

Decision – The risk management decision must include the safety risk assessment.   The risk assessment may be used to compare and contrast options or alternatives for system implementation.

The SMS Manual permits quantitative and qualitative assessments but states a preference for quantitative. It requires the assessments, to the maximum extent possible, to be scientifically objective, unbiased, and inclusive of all relevant data. Assumptions must be avoided when feasible. When assumptions must be made, they should be conservative in nature, and their basis should be clearly identified. As a decision tool, the risk assessment must be related to current risks and should compare the risks of various alternatives when applicable.

For each proposed change to the NAS, FAA Order 8040.4, Safety Risk Management, requires each LOB or Service Team to:

Perform and provide a risk assessment that compares each alternative considered (including no action/change or baseline) so that the alternatives can be ranked for decision-making.

Assess the costs and safety risk reduction or increase (or other benefits) associated with each alternative under final consideration.

Requirements of Comparative Safety Assessments (CSAs) may identify levels of additional safety risk for each of the alternatives, thereby affecting cost and schedule by requiring different levels of additional safety analyses to properly address the different risk levels.

2.2 AMS Policy

AMS policy is in Section 4.12 of the AMS. This SRMGSA and PSP are valuable sources for inputs to a Service Team's Implementation Strategy and Planning (ISP) document or other master planning documents, statements of work, and requirements. These documents are used by the Investment Analysis Team (IAT) to satisfy the requirement to implement a repeatable and disciplined process for conducting SRM in the acquisition of systems for the entire lifecycle of those systems. They include provisions for hazard identification, classification of risk, risk control, and acceptance.

2.3 SMS Manual

The SMS Manual provides a systematic and integrated method for managing the safety risk of ATC and navigation services in the NAS. The SMS requires that all organizations that have a role in providing ATC services (including those external to the ATO) identify and mitigate safety risk. Safety Risk Management Documents (SRMDs), Safety Risk Management Decision Memos (SRMDMs), safety incident reports, and safety inspection and evaluation reports provide managers with needed information regarding safety hazards and risks associated with systems (hardware and software), procedures,[3] and airspace designs.

Organizations are required to integrate SRM into their national and local activities and processes. the Office of Safety is responsible for facilitating SMS implementation across the ATO; managing SRM processes, procedures, and documents; facilitating SMS training; providing SRM expertise when necessary; auditing SRM processes; and evaluating the SMS.

The SMS provides a common framework to assess the safety risks of changes to the NAS. It addresses all aspects of ATC and navigation services, including airspace changes, air traffic procedures and standards, airport procedures and

---

[3] See Appendix M in the SMS Manual for a discussion on using the SRM process to assess risk incident to changes in ATC procedures.

standards, and new and modified equipment (hardware/software). The SMS facilitates cross-functional SRM among the ATC service providers and ensures intra-agency stakeholder participation in solving the safety challenges of an increasingly complex NAS. It is important to note that the SMS focuses on NAS safety, not employee safety. While employee safety is included as part of system safety analyses, it is considered only as it applies to, or affects, the NAS.

2.4   SRM for System Acquisitions

The AMS process applies primarily to the acquisition of systems and the evolution of legacy systems. It is robust enough to follow those systems through the JRC process, including the In-Service Decision (ISD) and deployment. It also addresses changes or modifications during re-baselining activities.

The SMS incorporates all AMS safety provisions but expands to allow the SRM process to address changes to air traffic operations, maintenance, airspace and procedures development, airports, new systems, and modifications to existing systems (hardware and software). For changes to an existing system that need to go through the configuration management process, FAA Order 1800.66, Configuration Management Policy, addresses how the NAS Change Proposal processes support the SMS. The SMS requires that all proposed changes to the NAS (e.g., new equipment; systems; modifications to existing equipment, systems and new and/or changes to existing procedures; operations) undergo SRM evaluation.   The SMS requires that SRM be performed early in the planning or change proposal process. SRM is a fundamental component of the AMS and the SMS — it ensures that safety-related changes are documented and resolved, whether the changes are to a component, a system, a procedure, or the NAS itself.

The JRC Secretariat depends on the SRM Office to independently concur that safety-related items on the JRC Readiness Criteria and Checklist (RCC) have been completed. The items apply to decisions by the JRC and subordinate boards on IA Readiness, Initial Investment Decision (IID), Final Investment Decision (FID), baseline changes, and the ISD. For the SRM Office to provide this independent concurrence, system safety documents and plans (such as SRMDs, PSPs, and non-safety documents with safety inputs such as the Investment Analysis Plan (IAP) and Program Requirements (PR)) are first brought to the ATO SSWG for review and subsequent concurrence by its chair. After final approval of these documents by the SRM Office, the JRC Secretariat is notified that the specific JRC checklist item has been completed.

2.5   SRM for Legacy System Acquisitions

SMS also applies to acquisition of changes to legacy systems. System safety focuses on legacy programs that are operational in the NAS as well as support programs that affect NAS operations (e.g., the En Route Information Display System, the Enhanced Back-up System, Traffic Flow Management - Modernization). Information gathered on changing legacy systems determines

what kind of system safety work is required to support the planned JRC decision. Legacy systems are not "grandfathered" under SMS. When a legacy system is subject to an Executive Council- (EC)- or JRC- approved change or baseline decision, or when the Service Team prepares to submit its next acquisition phase for JRC approval, the change is treated the same as a new system.

The system safety work for legacy systems usually involves some form of tailoring for various reasons:
- Programs are realigned or revised during development or implementation.
- Previous SRM decisions are no longer valid.
- Programs had previously advanced into the JRC process without SRM input or direction.

Tailoring builds on existing safety work and what must be done based on where the program is in the acquisition management lifecycle and past JRC decisions. Additional guidance on what analysis is required is given at the Safety Strategy meeting.

3.0 AMS/SMS PRINCIPLES

The SRM process is designed to mitigate safety risks throughout the NAS lifecycle of programs that modernize and upgrade the NAS. Its primary focus is to identify, mitigate, and control safety risks in the NAS. Each LOB or Service Team has unique responsibilities. However, the overall approach will remain the same: early identification and continuous control of those hazards that introduce high risk into the NAS. The following paragraphs summarize the SRM process and tasks the Service Teams must accomplish in the AMS.[4] The "Bow-Tie Model" illustrated in Appendix A is commonly used for conducting hazard analysis.

3.1   SRM Process

A systematic SRM process has five general phases:[5]
- Describe the system.
- Identify the hazards.
- Analyze the risk.
- Assess the risk.
- Treat (mitigate) the risk.

3.1.1 Definitions

Causes
A cause is an event that results in a hazard or failure. A crimped fuel line or water in a fuel tank is an example. In many systems, these events may result in "loss of engine power" (hazard). Causes can occur by themselves or in combinations.

Hazard
A hazard is any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. A hazard is a condition that is a prerequisite to an accident or incident. A "loss of engine power," under certain conditions or system states may result in injury of death.

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

The SMS Manual defines a system as "an integrated set of constituent pieces that are combined in an operational or support environment to accomplish a defined objective. These pieces include people, operational environment, usage,

---

[4] Criteria for the AMS SRM decision process are found in the SMS Manual and in Figures 5.1-1 and 5.1-2 of this document.
[5] Chapter 3 of the SMS manual elaborates on what constitutes these five phases.

equipment, information, procedures, facilities, services, and other support services."

System state can be described in operational/procedural terms (e.g., Visual Flight Rules vs. Instrument Flight Rules, Instrument Landing System approach), conditional terms (e.g., Instrument Meteorological Conditions vs. Visual Meteorological Conditions, low altitude, rough terrain) or physical terms (e.g., Electromagnetic Environment Effects, heavy precipitation, low air speed, no hydraulic pressure, high drag).

For any given hazard (e.g., loss of power from an engine), not all system states have equal weight. For example, loss of one engine (for a multi-engine aircraft) at high "Above Ground Level" altitude and airspeed is not likely to result in a catastrophic accident. Most multi-engine aircraft are designed to fly on one engine in a restricted flight envelope. However, loss of one engine in some system states (low airspeed, low altitude, high gross weight) has the potential to result in loss of control or lift. In such a system state, the hazard would be catastrophic. The SMS Manual requires the assessment to consider the worst case system state. Any given hazard may have a different risk level in a different system state. Hazard assessment must consider all possibilities, from the least to the most likely, allowing for "worst case" conditions. It is important to capture all system states to identify worst credible outcomes and unique mitigations.

Effect and Severity

The effect is a description of the potential outcome or harm of the hazard if it occurs in the defined system state. Severity is the measure of how bad the results of an event are predicted to be. In other words, hazard plus system state equals effect or severity. The hazard's effect or severity will vary depending on the system state selected. The hazard severity ranges from 1, Catastrophic, to 5, Minimal, as shown in Table 3.2-1. For example, the effect is the result of what happens if the loss of engine power occurs at low altitude, low airspeed, and high gross weight. The potential effect in this case would probably be catastrophic. Therefore, this hazard would be rated as "1, Catastrophic" (see Table 3.2-1 in this document).

Likelihood

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

> Determine how often the hazard is expected to occur. This can be a quantified or qualitative estimate. Usually, it is a function of the likelihood of the combinations of the cause(s). Sometimes, this can be determined by evaluating incident or accident databases to see how often the hazard has been recorded in the field.

3.2 Risk Assessments in the AMS

Risk assessments conducted to support the AMS must comply with the guidelines established in the latest version of the SMS Manual. Use the definitions in Tables 3.2-1 and 3.2-2 for SRM in the AMS.

Table 3.2-1: Severity Definitions

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

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

1 – As defined in the 2005 Runway Safety Report

2 – As defined in FAA Order 7210.56, *Air Traffic Quality Assurance*, and Notice JO 7210.663, *Operational Error Reporting, Investigation, and Severity Policies*

3 – Minor Injury - Any injury that is neither fatal nor serious.

4 – Serious Injury - Any injury which: (1) requires hospitalization for more than 48 hours, commencing within seven days from the date the injury was received; (2) results in a fracture of any bone (except simple fractures of fingers, toes, or nose); (3) causes severe hemorrhages, nerve, muscle, or tendon damage; (4) involves any internal organ; or (5) involves second- or third-degree burns, or any burns affecting more than five percent of the body surface.

5 – Fatal Injury - Any injury that results in death within 30 days of the accident.

Note:
- Once hazard severity has been established in the Operational Hazard Assessment, it does not change without sufficient justification and ATO SSWG Concurrence.
- Evaluate hazard severity as it relates to the NAS, not to employee safety.

Calculating Likelihoods

1. To arrive at a quantitative estimate of the likelihood of a given effect or severity occurring for the example of loss of an engine in a given system state, assume that the likelihood estimate for the loss of one engine is 0.001 per operational hour.

2. Estimate the likelihood of the worst-case system state. This estimate can also be quantified or qualitative. For many systems, the Operational Services Environment Description will provide many clues in developing this answer. For this example, assume that the

likelihood of being in the worst case system state (low altitude, low airspeed, high gross weight) is 0.001 per operational hour.

3. For the effects to be manifested in the worst case, both the hazard (loss of power) and the worst case system state (low altitude, etc.) must occur at the same time. The likelihood of this occurrence can be estimated by multiplying 0.001 x 0.001. In this example, the estimate would be 0.000001, or 1×10^{-6} per operational hour. Using the definitions in Table 3.2-1, the likelihood would be characterized as "Remote."

4. The severity (1, Catastrophic) combined with the likelihood estimate (C, Remote) is an estimate of the risk. The risk is expressed as a Risk Assessment Code (RAC), or in this example, a "1C (HIGH)."

Use the following principles with this model:

- Risk is the composite of predicted severity and likelihood of the potential effect of a hazard in the worst credible system state.
- Severity is determined by the worst credible potential outcome. Less severe effects may also be analyzed, but at a minimum, the most severe effects must be considered. Severity is independent of likelihood. (DO NOT consider likelihood when determining severity.) However, the determination of likelihood is dependent on severity. Likelihood is determined by how often the resulting harm can be expected to occur at the worst credible severity.
- Hazards are composed of one or more causes.
- Causes can be technical and/or procedural in nature.
- The system state refers to a variety of hazardous system conditions, including, but not limited to, location, mode, velocity, operating rules in effect, type of operation, energy, operational environment, and ambient environment.
- When using terminology, be consistent with the definitions in this document and in the SMS Manual, including those for accidents and incidents. An accident is defined as "an unplanned event that results in a harmful outcome; e.g., death, injury, occupational illness, or major damage to or loss of property." An incident is defined as "a near miss episode with minor consequences that could have resulted in greater loss An unplanned event that could have resulted in an accident, or did result in minor damage, and indicates the existence of, though may not define, a hazard or hazardous condition."[6]

---

[6] See Appendix A of the SMS Manual for a complete list of definitions.

Table 3.2-2: Likelihood Definitions

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

The following Risk Matrix, Figure 3.2-1, shows risk as a composite of severity and likelihood. This matrix classifies risk into three levels: High, Medium, and Low. These levels define how the FAA AMS and SMS process conduct risk resolution for each identified hazard in accordance with Figure 3.2-2.

Note: Risk is defined as risk to the NAS, not risk to the employee.

Figure 3.2-1: Risk Matrix

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

* Unacceptable with Single Point and/or Common Cause Failures

High Risk	Red
Medium Risk	Yellow
Low Risk	Green

High risk – Unacceptable risk; change cannot be implemented unless the hazard's associated risk is mitigated so that risk is reduced to a medium or low level and AOV approves the mitigating controls. Tracking, monitoring, and management are required.

Medium risk – Acceptable risk; minimum acceptable safety objective; change may be implemented, but tracking, monitoring, and management are required.

Low risk – Acceptable without restriction or limitation; hazards are not required to be actively managed but are documented.
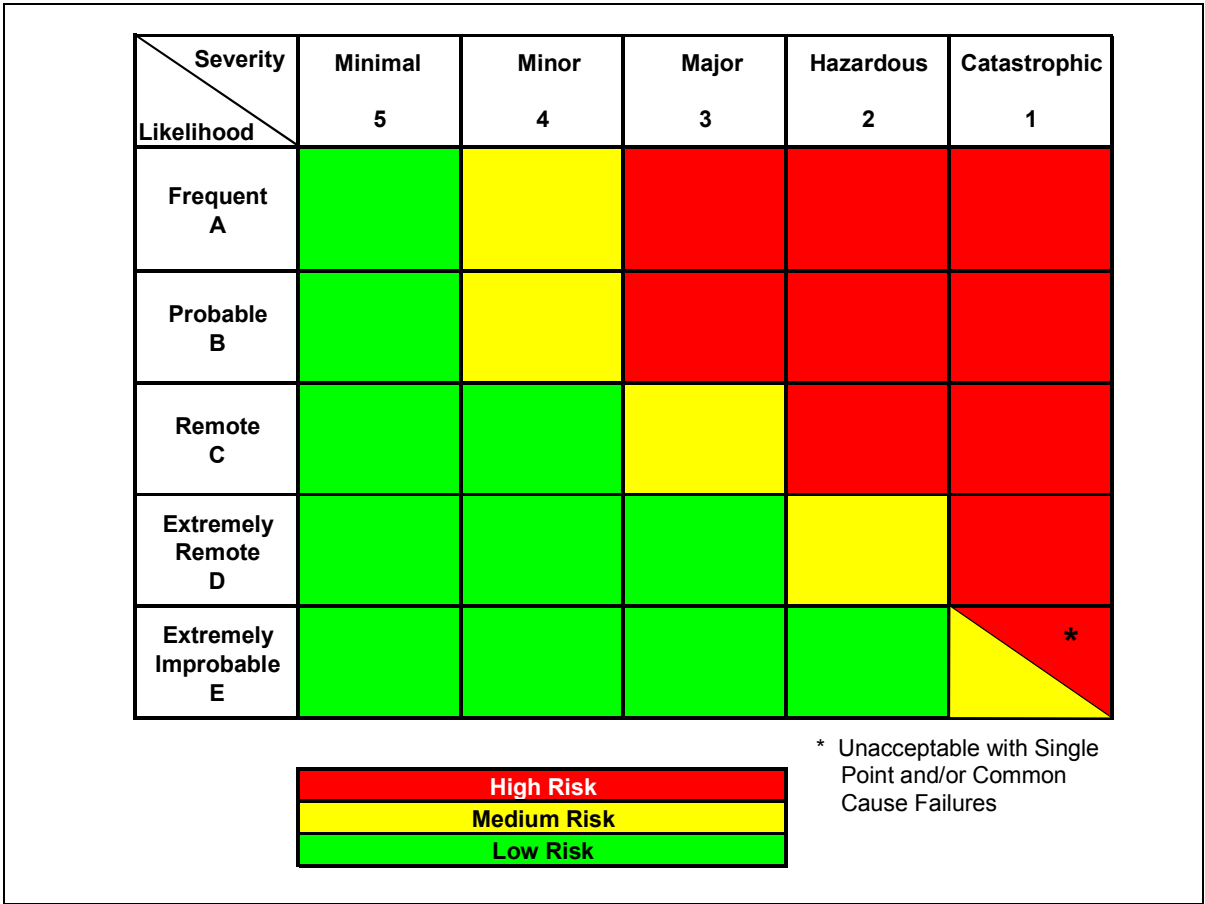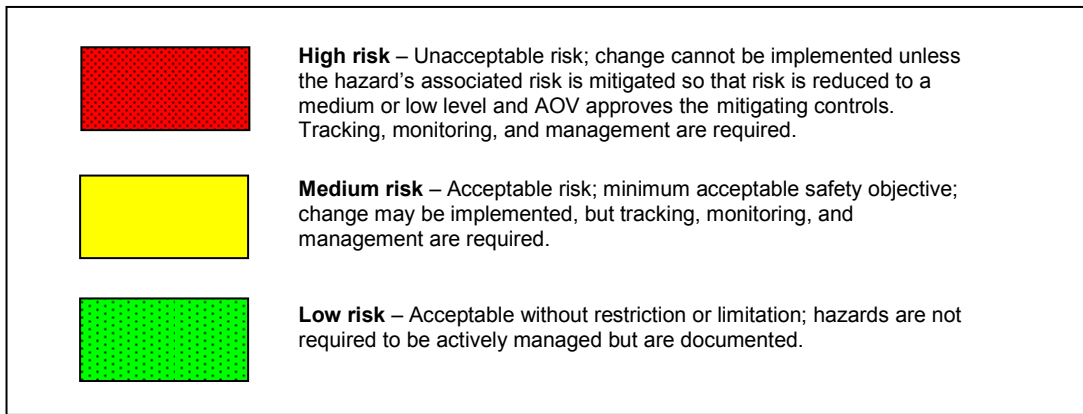
Figure 3.2-2: Risk Acceptance Criteria

3.2.1 Types of Risk

The SMS Manual categorizes risk into four types: *initial risk, current risk, predicted residual risk, and residual risk.*

- *Initial risk* is the severity and likelihood of a hazard when it is first identified and assessed. This category is used to describe the severity and likelihood of a hazard in the beginning or preliminary stages of a proposed change or analysis. Initial risk is determined by considering verified controls and assumptions made about the system state. When assumptions are made, they must be documented. The initial risk does not change once the analysis is complete.

- *Current risk* is the predicted severity and likelihood of a hazard at the current time. When determining current risk, validated and verified controls can be used in the risk assessment. Current risk may change based on the actions taken by the decision-maker that relate to the validation and/or verification of the controls associated with a hazard. The Current Risk may be formally changed by submitting the requirements verification evidence to the ATO SSWG for the Safety Action Record (SAR). *(additional clarification is provided below on the use of current risk)*

- *Residual risk* is the risk that remains after all control techniques have been implemented or exhausted and all controls have been verified. Only verified controls can be used to assess residual risk.

- *Predicted residual risk* is used when conducting an analysis prior to formal verification of requirements or controls. It is based on the assumption that validated and recommended safety requirements will be verified.

Current risk and predicted residual risk statuses are entered into the FAA Hazard Tracking System (HTS). Current risk is used to show the risk if the existing validated and verified controls are all considered. When determining current risk, the Safety Engineer assesses both validated and verified requirements/controls in the risk assessment. However, recommended controls are not included. This shows the decision-makers the potential effect if recommended safety requirements are not implemented. The Service Team may take actions relating to the validation and/or verification of the controls associated with a hazard description, and the current risk may change as a result.

Predicted residual risk is the risk status predicted to occur when recommended controls are both validated and verified. This risk rating is a tool for the Service Team to develop the system with an acceptable level of risk.

The following guidelines should be used in determining the status of recommended safety requirements:

- *Safety requirements* are used to control hazards and are documented in the Service Team's Safety Requirements Verification Table (SRVT). All safety requirements must be identified in the PR document. Changes to safety requirements must be reported to the Service Team and, if necessary, to the ATO SSWG before they are modified or deleted.

- ***Recommended safety requirements*** are requirements that the safety engineer determines could mitigate a hazard; however, they are not yet validated requirements. (These recommendations can also be referred to as *candidate safety requirements* until validated by the Service Team.) Once they have been validated, the *recommended safety requirements* become *validated safety requirements.* Recommended safety requirements associated with a hazard description are maintained in the HTS until they have been validated and verified.

3.3   Safety Order of Precedence

Programs in the AMS and ATO should use the safety order of precedence in Table 3.3-1 to select controls and requirements as described in section 3.11.9 of SMS Manual 2.1.

Table 3.3-1: Safety Order of Precedence

Description	Priority	Definition	Example
Design for minimum risk.	1	Design the system (e.g., operation, procedure, or equipment) to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level through selection of alternatives.	1. If a collision hazard exists because of a transition to a higher Minimum En Route Altitude at a crossing point, moving the crossing point to another location eliminates the risk. 2. If "loss of power" is a hazard to a system, adding a second independent power source reduces the likelihood of the hazard.
Incorporate safety devices.	2	If identified risks cannot be eliminated through alternative selection, reduce the risk via the use of fixed, automatic, or other safety features or devices, and make provisions for periodic functional checks of safety devices.	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 effects. Warnings and their application are designed to minimize the likelihood of inappropriate human reaction and response.	1. A warning displayed on an operator's panel 2. "Engine Failure" light in a helicopter 3. Flashing Minimum Safe Altitude Warning or Conflict Alert Indicator on a radar screen
Develop procedures and training.	4	Where it is impractical to eliminate risks through alternative selection, safety features, and warning devices,: procedures and training are used. However, concurrence of management authority is required when procedures and training are solely applied to reduce risks of catastrophic or hazardous severity.	1. A missed approach procedure 2. Training in stall/spin recovery 3. Procedure to vector an aircraft above a Minimum Safe Altitude on a Very High Frequency Omni-directional Range airway 4. Procedures for loss of communications

3.4   Safety Decision and Analysis Documentation

3.4.1   SRMDs

SRMDs thoroughly describe the safety analysis for a given proposed change. They document the evidence to support whether or not the proposed change to the system is acceptable from a safety risk perspective. SRMDs are kept and maintained by the organization responsible for the change for a period equivalent to the lifecycle of the system or change. The SRMDs expand with

each assessment or analysis as a program moves through the AMS lifecycle. When the Service Team determines that specific safety analyses are required, the analyses are documented and become part of the SRMD. The documents are listed in Table 3.4-1. Each Service Team must maintain an SRMD as a record of the progress of the program. As shown in the SMS Manual (Chapter 3), SRMDs contain the following elements:

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

3.4.2 SRMDMs

If the change is not expected to introduce safety risk into the NAS, there is no need to conduct further safety analysis; instead, the change proponent documents that determination, along with the justification for the decision as to why the change is not subject to the provisions of additional SRM assessments and supporting documentation beyond the initial safety analysis in an SRMDM.

The ATO SSWG reviews the SRMDM for acquisitions. Upon concurrence by the SSWG Chair, it is kept on file for the lifecycle of the change.

3.4.3 Other Documentation

- SARs - All hazards must be entered into the FAA HTS. The SARs contain all of the hazards that must be tracked throughout the lifecycle. The Service Team should periodically update the SAR to identify actions taken to validate and verify the safety requirements for each hazard.

- The PSP is a plan to integrate the execution of SRM into an individual program. The SRVT is a living safety requirements document that identifies and tracks safety requirements on a program, along with the validation and verification status of each requirement. The System Safety Program Recommendations (SSPR) is a means of transmitting a summary of recommendations from the safety analysis team to the Service Team.

System safety documents are listed in Table 3.4-1.

Table 3.4-1: List of System Safety- Related Documents in Acquisitions

Document	SRMGSA paragraph
Operational Safety Assessment (OSA)	K.1
Comparative Safety Assessment (CSA)	K.2
Preliminary Hazard Assessment (PHA)	K.3
Preliminary Program Requirements (pPR), Section 14	Reference the FAA Acquisition System Toolset (FAST)
IAP	Reference FAST
PSP	K.4
System Safety Program Plan (SSPP)	K.4
Sub-System Hazard Analysis (SSHA)	K.5
System Hazard Analysis (SHA)	K.6
Operating and Support Hazard Analysis (O&SHA)	K.7
Test Safety Analysis (TSA)	K.8
System Safety Assessment Report (SSAR)	K.9
SRVT	K.10

4.0 AMS SRM TASKS

This section details the tasks and organizational roles and responsibilities for conducting SRM in the AMS.

All of the SRM products specified in this section must comply with the guidelines specified in the SMS Manual. Review and concurrence by the ATO SSWG is required.

4.1 The FAA Lifecycle Management Process

The FAA executes its acquisition management policy using the lifecycle management process, which is organized into a series of phases and decision points as shown in Figure 4.1-1. The circular representation conveys the principle of seamless management and continuous improvement in service delivery over time. Application is flexible and may be tailored as appropriate. Section 2 of the AMS policy, Lifecycle Management Phases and Decision Points, contains detailed policy on the lifecycle management process.
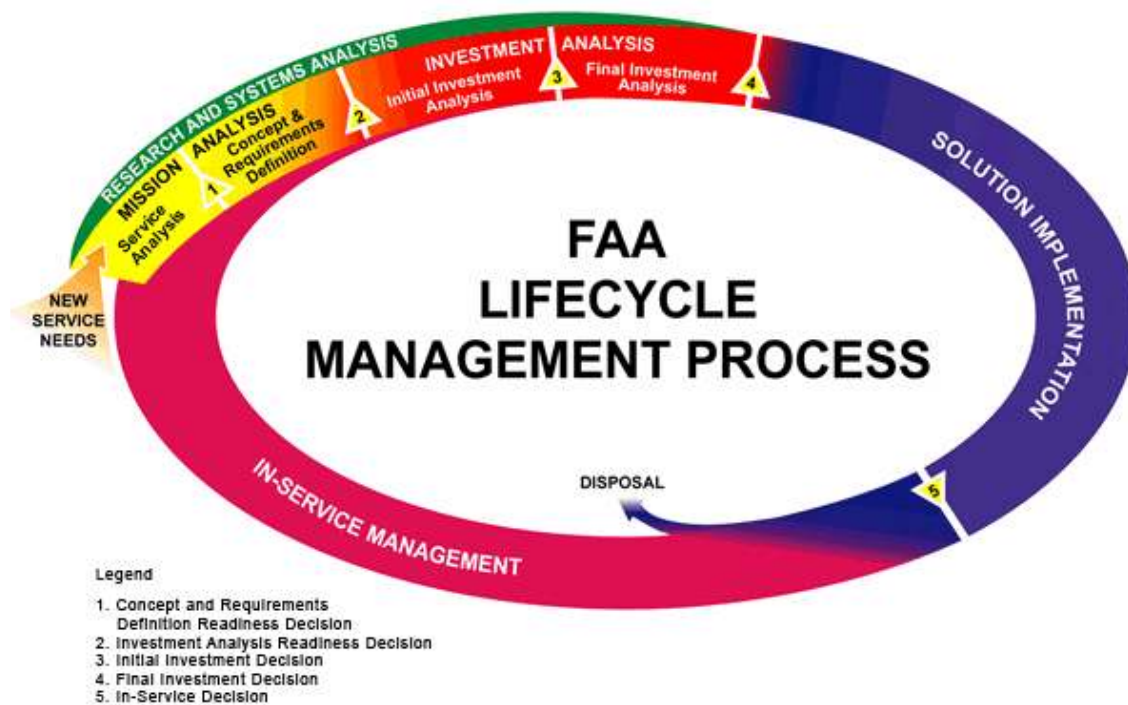

Figure 4 .1-1: FAA Lifecycle Management Process

The basis for initiating NAS changes differs for each organization. The level at which SRM is conducted will also vary by organization and/or proponent, as well as by the type of change. SRM is carried out at the national level for major system acquisitions. It is performed at the regional or local level to address proposed changes to equipment or ATC procedures.

The Safety Analysis Decision Chart (Figure 4.1-2) shows when the various SRM-related tasks should be completed and by whom. This chart helps Service Teams determine the type and scope of the system safety program required.

Acquisition Phase	AMS Decision Point	Type of Analysis Required	Documentation Needed *ATO SSWG reviews and concurs with all safety documentation.*	Responsibility for Preparation
Service Analysis	CRD Readiness Decision	Operational Safety Assessment (OSA)	Initiate SRMD: OSA as soon as enough information is available on Functional Requirements[1]	Service Unit Sponsor[2]
Concept and Requirements Definition	Investment Analysis Readiness Decision		Approved SRMD: OSA, pPR Section 14, Investment Analysis Safety Section, ISP Safety Section	
Initial Investment Analysis	Initial Investment Decision	Comparative Safety Assessment (CSA)	SRMD: CSA (Update to the existing SRMD) Results input to Business Case Analysis Report and briefed to EC and JRC as appropriate in SRMGSA format	Service Team Service Team's BCAT provides input
Final Investment Analysis	Final Investment Decision	Preliminary Hazard Analysis (PHA)	SRMD: PHA (Update to the existing SRMD) PSP[3] JRC Readiness Checklist OK	Service Team
Solution Implementation	In-Service Decision	Sub-System Hazard Analysis (SSHA) System Hazard Analysis (SHA) Operating & Support Hazard Analysis (O&SHA) Others as defined in the Program Safety Plan (PSP)	Update existing SRMD to include: SSHA, SHA, O&SHA SSAR (includes Safety Action Records and SRVT) ISR Checklist Complete	Service Team

General Note: Order of completion for some of the safety analyses is not necessarily serial, some of these may start as soon as information is available
Note 1: An early Safety Strategy Meeting may tailor this out as Not Applicable for the CDR Readiness Decision
Note 2: The SRM Office Representative reports the CRD, IA, and ISD safety needs and their status at the JRC Readiness Meeting
Note 3: The PSP should describe the Contractor's System Safety Program requirements and the types of analyses in the Contract Data Requirements List

Figure 4.1-2 Safety Analysis Decision Chart

4.2   SRM Tasks in the AMS

A major objective of this document is integrating SRM into the AMS process. This objective will be achieved by accomplishing SRM tasks using the right system safety tools and techniques at an appropriate time to support the decisions made in the lifecycle phase. These tasks are performed by the OSUs and result in products packaged in SRMDs, which are reviewed and approved prior to a JRC decision. These tools and their application to the lifecycle AMS process are depicted below in Figure 4.2-1.
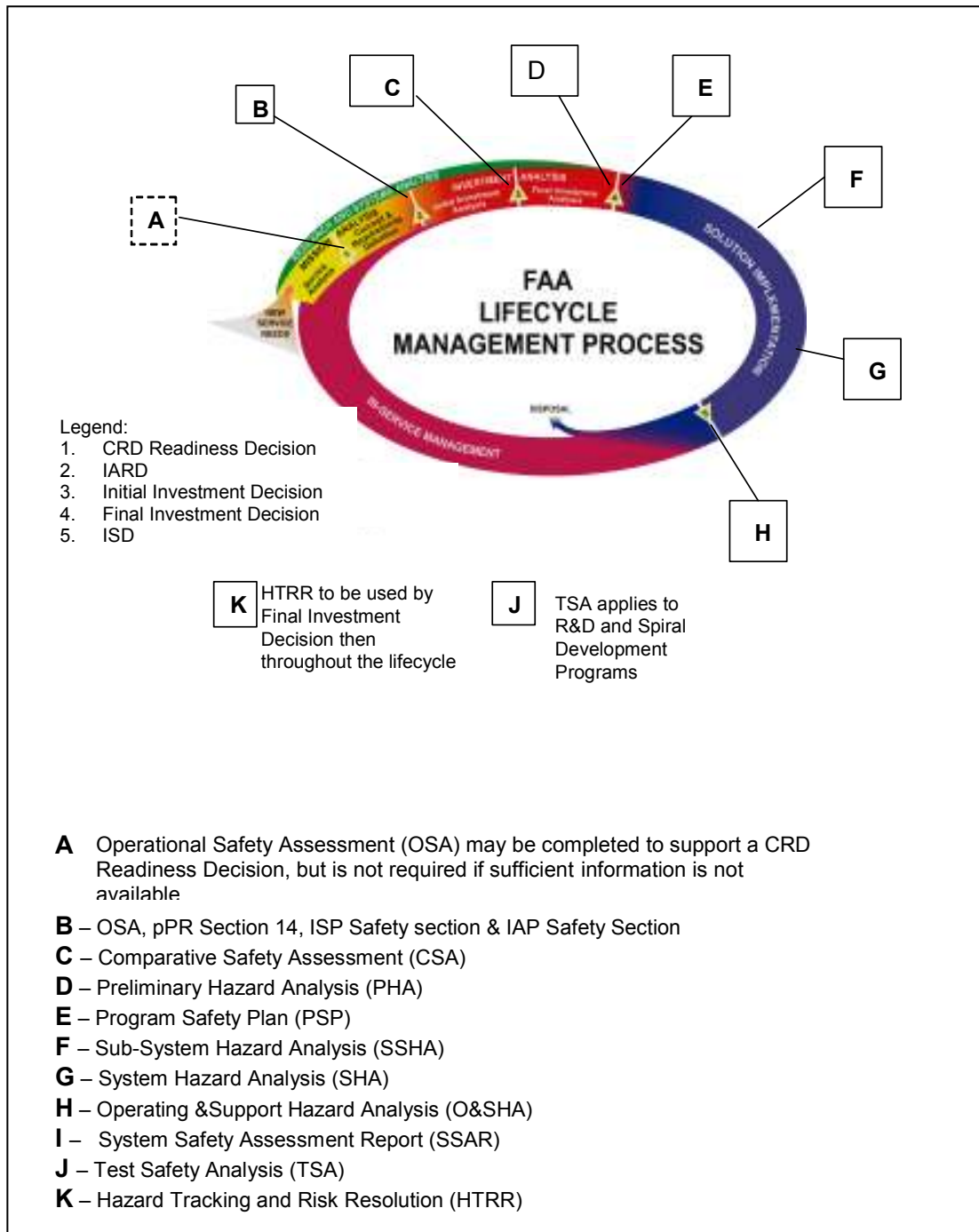
Legend:
1. CRD Readiness Decision
2. IARD
3. Initial Investment Decision
4. Final Investment Decision
5. ISD

K HTRR to be used by Final Investment Decision then throughout the lifecycle

J TSA applies to R&D and Spiral Development Programs

A Operational Safety Assessment (OSA) may be completed to support a CRD Readiness Decision, but is not required if sufficient information is not available

B – OSA, pPR Section 14, ISP Safety section & IAP Safety Section

C – Comparative Safety Assessment (CSA)

D – Preliminary Hazard Analysis (PHA)

E – Program Safety Plan (PSP)

F – Sub-System Hazard Analysis (SSHA)

G – System Hazard Analysis (SHA)

H – Operating &Support Hazard Analysis (O&SHA)

I – System Safety Assessment Report (SSAR)

J – Test Safety Analysis (TSA)

K – Hazard Tracking and Risk Resolution (HTRR)

Figure 4.2-1: SRM and System Lifecycle

When the Safety Analysis Decision Chart shown in Figure 4.1-2 is used to determine if an in-depth safety analysis is required, the decision will identify the necessary analyses. (As discussed in section 2.5, tailoring may be required for legacy programs entering the AMS.) The various analyses typically conducted are discussed in Appendix K.

SRM Timelines

The ATO EC or an Associate/Assistant Administrator of the (non-ATO) LOB makes the Investment Analysis Readiness Decision. To support this decision, OSAs, SRM inputs to the pPR and IAP, or completed SRMDMs must be completed and approved at least 30 to 50 days before the EC meeting.

The IID, FID, and ISD have several milestones: the JRC meeting, the EC briefing that comes about two weeks before each JRC meeting, and the Business Case Analysis Report (BCAR), which replaced the IA Report. The IA inputs (e.g., the pPR, Final PR, programmatic safety assessment) are completed well before the BCAR itself. The BCAR is a Service Team product that occurs about 10 days before the EC briefing for each JRC decision point. It includes line items for supporting tasks and assessments, including those for system safety, such as the CSA and PHA. The PSP should also be listed as a product. Briefings prepared for an ISD should include the results of the SSAR.

Each program needs to allow sufficient time prior to the 11-week review with the SSWG to produce a quality SRMD. Depending upon the complexity, this may be from 1 month to 1 year prior to commencing the SSWG review process. This should be included in the PSP and reviewed with the SSWG Chair.

Figure 4.2-2 shows an average timeline for the process. Complex SRMDs may require longer review intervals or multiple reviews.
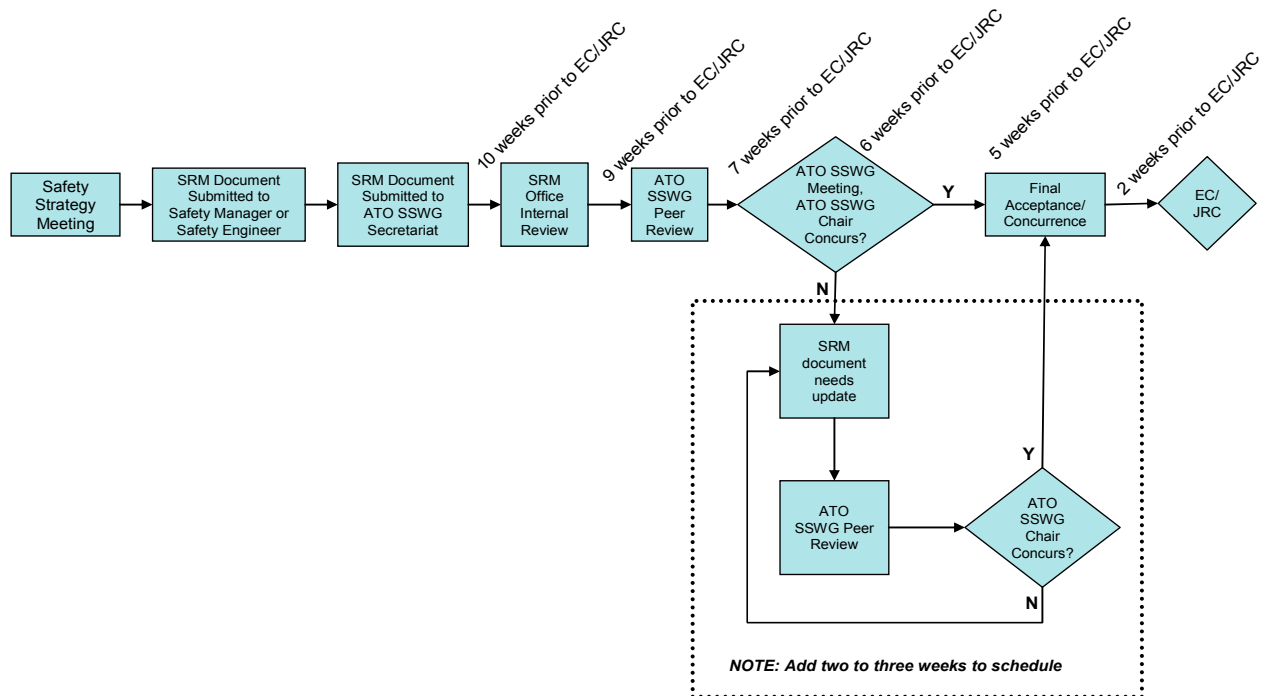
Figure 4.2-2: SRM Documentation Timeline

4.2.1 Safety Documentation

Appendix K contains a discussion of each of the assessment and analysis types, as well as other required documentation for each phase of the lifecycle.

4.2.2 Hazard Tracking and Risk Resolution (HTRR)

HTRR is a closed-loop means of ensuring that the requirements and mitigations associated with each hazard that has associate MHR Each program must use the FAA HTS throughout the decision process to accomplish HTRR. Approved users can access the FAA HTS on the FAA Intranet. There are two versions on the web site: one for system acquisitions and one for operations. The FAA HTS contains hazards associated with changes to the NAS that require SRM. It is not intended for accident/incident reporting.

Service Teams must ensure that:

- When a safety analysis is completed or an incident analysis identifies a hazard, all identified hazards are entered into the HTS. (Environmental,

Energy, and Occupational Safety and Health hazards are only included if they impact the NAS.)

- Each hazard is recorded in a unique record (i.e., an SAR) in the HTS.

1. Medium and High Risk hazards are tracked to closure prior to the ISD. However, all safety requirements (including those for low risk hazards) must be validated and verified.

Each SAR includes:

1. A description of the hazard status
2. An updated narrative history of changes to the SAR (e.g., verification status changes)
3. A current risk assessment
4. A rationale for the risk severity and probability, including existing controls and SRVT requirements
5. A mitigation and verification plan for each safety requirement
6. Potential effects if the hazard is realized

Each SAR must be classified according to status in accordance with Table 4.2-1, below. The ATO SSWG will review all program SARs with proposed status, open status, and current High Risk. This review will occur at least twice a year for each program.

The SRM Panel determines the RAC, which the ATO SSWG reviews. (If the SSWG disagrees with a RAC and the disagreement cannot be resolved, the SSWG will prepare a memo for the Director of SMS's signature to the appropriate SU, and the SRMD will not gain concurrence.)

The status of each SAR is defined by the guidelines in Table 4.2-1. Status information is used to brief management at ISD and appears in the SSAR.

Table 4.2-1: SAR Status Definitions

Status	Definition
Proposed	The hazard has been identified, and the SAR has been written. The SAR has not been reviewed or approved by the ATO SSWG.
Open	The SAR has been approved by the ATO SSWG. Mitigation and verification plan have not been developed.
Monitor	The SAR has been approved by the ATO SSWG. A mitigation and verification plan for the SAR exists and has been approved by program management. Results of the mitigation and verification plan are forthcoming.

Status	Definition
Recommend Closure	All mitigation and verification actions are complete. The SAR is awaiting review by the ATO SSWG, Status and residual risk will then be determined.
Closed	No further action is needed. The SAR is closed by the ATO SSWG and forwarded to Director of SMS for review and coordination of risk acceptance by the appropriate management activity.

4.3   Software Safety

Since the advent and expansion of computers, the safety community has worked to design safety into systems influenced by software and firmware. The safety community has implemented software safety to mitigate the additional risk of having computing systems and software- or firmware-controlled devices operate and control safety-critical functions. (For the remainder of this section, all references to software include software and firmware, unless specifically stated.) Any software that performs, influences, informs, or interacts with system safety-critical functions or operations must undergo the focused Software Safety Analyses (SwSAs). Those analyses are intended to ensure that any anomalous software behavior on safety-critical functions or operations is properly mitigated.

Attaining a safe and effective system solution is the result of a system safety program. Software safety assurance provides the confidence that system safety requirements implemented in, and by, software function as intended. Software assurance does not in and by itself ensure system safety. It only provides a level of confidence that the software's potential for anomalous behavior has been identified and mitigated.

Software Safety Assessments

SwSAs are detailed hazard evaluations of the system software and firmware to identify hazards incident to safety-critical operator information, management, and control functions identified by the appropriate system safety analyses listed in Appendix K. SwSAs ensure that procedural errors and malfunctions of any software or firmware modules do not cause or contribute to a failure condition.

Various analysis techniques and methodologies (e.g., software/system fault tree analysis, software sneak analysis, design walkthroughs, code walkthroughs, cross reference-listing analysis) are used for SwSAs. Each SwSA will be integrated into the appropriate System Hazard Analysis. Updates to the system safety analysis will be performed and documented if the SwSA uncovers any additional hardware/system-related safety hazards.

4.4   Software Assurance Level (SwAL) Assignment Matrix

The SwAL Assignment Matrix in Figure 4.4-1 establishes a level of rigor the software development process needs to satisfy to ensure that the software operates safely within a systems context. Integrity, continuity of service, and

assurance that the software will not contribute to a failure condition are the end products of the software safety and software assurance processes.

To permit full integration and harmonization between the Airborne and CNS/ATM safety communities, an approach for selecting SwALs has been adopted. This approach is compatible and acceptable to both communities without degrading end-to-end system safety. If the software of any NAS system directly influences an aircraft system, it must comply with, and be considered acceptable to, the airborne certification authority. RTCA/DO-178B has been invoked as an acceptable means, but not the only means, of compliance for securing FAA approval of digital computer software. Table 4.4-1 defines the association between CNS/ATM SwALs and Airborne assurance levels, as specified in RTCA/DO-278.

RTCA/DO-178B bases the selection of SwALs purely on severity as it relates to the aircraft (e.g., catastrophic failure condition for the aircraft). Typically, software is specific to the application and does not present the reliability parameters and historic lifecycle data found with hardware. The likelihood of software's anomalous behavior is difficult to determine since true historical data do not exist. Therefore, in the DO-178B methodology, likelihood must be considered probable. RTCA/DO-178B effectively uses a one (likelihood of probable) by five (severity) matrix for determining the SwAL required to mitigate the anomalous behavior of software contributing directly to a hazard affecting aircraft operations. The first row in Table 4.4-1 illustrates the RTCA/DO-178B determination of the assignment of Assurance Levels within the CNS/ATM SwAL Assignment Matrix and its complement translation to RTCA/DO-278.

Table 4.4-1: CNS/ATM to Airborne Level Association

DO-278/ED-109 Assurance Level	DO-178B/ED-12B Software Level
AL 1	A
AL 2	B
AL 3	C
AL 4	No Equivalent
AL 5	D
AL 6	E

Because the goal of FAA programs is to ensure the safety of the flying public, a consistent approach to the selection of SwALs is an absolute necessity. Additionally, since federal law governs aircraft safety, interfacing ground-based systems must comply with the airborne selection of a SwAL. For example, when the airborne element of an integrated ground-based/airborne system is

developed to an assurance level of "C," the ground-based complement must be developed to an equivalent level of "3."

Table 4.4-2: SwAL Assignment Matrix

DO-178B	DO-278	Initial risk rating from PHA in which software contributes to system-level hazard
A	AL 1	1A, 1B ←
B	AL 2	1C, 2A, 2B ←
C	AL 3	1D, 2C, 3A, 3B ←
–	AL 4	1E, 2D, 3C, 3D ←
D	AL 5	2E, 3E, 4A, 4B, 4C, 4D ←
E	AL 6	4E, 5A, 5B, 5C, 5D, 5E ←

Notes:
1. Minimally recommended software assurance levels are based on system risk. Any deviation must be pre-approved by the appropriate approval/certification authority.
2. DO-278 equates to DO-178B for software whose functionality has a direct impact on aircraft operations (e.g., Instrument Landing System, Wide Area Augmentation System).

4.5   Equivalent Processes

Every program is different in scope, complexity, criticality, and resources. In recognition of this, programs may use other equivalent processes for conducting the hazard analysis phase of SRM. While these processes may be used, the minimum requirements set forth in this document must still be met. Table 4.5-1 lists the equivalent safety analyses processes that may be used instead of the hazard analyses described in this guidance. One may be used under the following conditions:

2. The equivalent process must meet the minimum requirements for the safety analyses outlined in this document.
3. The equivalent process must be described in the PSP.

For additional descriptions of the equivalent processes between air traffic and certification, see Appendix L.

Table 4.5-1: Equivalent Processes

SRMGSA Analysis	Equivalent Analysis	Equivalent Process Document
OSA	Functional Hazard Assessment (system level and aircraft level)	ARP4761 (1996-12). Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment. Available from SAE. Para 3.1, 3.2, and Appendix A.
PHA	Preliminary System Safety Assessment	ARP4761 (1996-12). Available from SAE. Para 3.1, 3.3, and Appendix B.
SSAR including the SSHA	System Safety Assessment	ARP4761 (1996-12). Available from SAE. Para 3.1, 3.4, and Appendix C.
SHA	Common Cause Analysis composed of Particular Risk Assessment, Zonal Safety Analysis, and Common Mode Analysis	ARP4761 (1996-12). Available from SAE. Para 4.4, and Appendix I (Zonal Safety Analysis), Appendix J (Particular Risk Assessment), and Appendix K (Common Mode Analysis).

4.6   Continuous Monitoring During ISM

Chapter 4 of the SMS Manual address Safety Assurance and Evaluation and Safety Data Tracking and Analysis. The activities defined in these chapters are designed to meet an International Civil Aviation Organization, Office of Air Traffic Safety Oversight (AOV), requirements to measure the effectiveness of the safety requirements, controls, and mitigations that have been implemented for hazards with low or medium residual risk. To meet this objective, Service Teams develop metrics related to the requirements for the identified hazards and collect the appropriate data to analyze the effectiveness of the mitigations. Service Teams then conduct trend analysis to determine if the implemented controls are effective in reducing the likelihood of incidents and accidents.

5.0 ORGANIZATION, ROLES, AND RESPONSIBILITIES

5.1 Organization Objectives

The organization, roles, and responsibilities involved in AMS SRM are designed to ensure that the following objectives are met:
1. Systems under consideration for inclusion in the NAS are evaluated systematically and at an appropriate time to assist in decision-making.
2. Appropriate safety requirements are developed for each system using best system engineering practices in the earliest possible phases of system development and consistent with the AMS.
3. Hazards are identified, assessed for risk, and, if necessary, actively controlled and mitigated to an acceptable level of risk.
4. Consideration of safety risk is an integral part of each AMS decision and is required for every JRC decision in which resources are committed to development and acquisition of systems.
5. FAA resources are properly focused on controlling and mitigating the highest risk elements and hazards of the NAS and the systems under development.

To accomplish these objectives, the organization proposing a change to the NAS must commit the required resources to ensure that the following steps are completed for each program:

Safety Strategy Meeting – The Service Team meets with the Office of Safety to determine the safety effort required for the proposed initiative.   This meeting is led by the ATO SSWG Chair and needs to be supported by the Safety Manager or Safety Engineer from the Service Unit. If a Service-Level MA effort is to take place, a representative from this group should coordinate a Safety Strategy meeting with the Office of Safety through the Safety Manager or Safety Engineer.

Safety Plan – The product of the Safety Strategy meeting (as agreed to by the ATO SSWG Chair) is documented in the following documents: preliminary Program Requirements Section 14, IAP, Concept and Requirements Definition (CRD) Plan. At the end of the MA phase, the IAP and pPR are updated to reflect the planned safety effort during the IA phase. The plan is consistent with the latest version of the SMS Manual and this document.

Hazard Identification – The hazard analyses and assessments must identify the NAS safety risks associated with the system or operations being evaluated.

Hazard Classification through Analysis – The risks must be characterized in terms of severity of consequence and likelihood of occurrence.

Risk Assessment – The risk assessment of the hazards examined must be compared to the acceptability criteria specified and the results provided in a manner and method easily adapted for decision-making.

Decision – Program decisions must be evaluated for their impact on the safety of the system. Those with safety impacts must include the safety risk assessment.

Figure 5.1-1 shows the overall plan for conducting SRM in the AMS. It shows the decision points, tasks (or analysis type), and responsible organizations.

Safety
Strategy Meeting   IARD   IID   FID   ISD

Responsibility	MA Phase	IA phase	IA phase	SI phase	ISM
Service Team	Develop SafetyPlan (1) SRMDM (2) SRMD: OSA	SRMD: CSA (3)	PSP SRMD: PHA (4)	(Accepts SSPP)	Provide Status Reports
Service Team and Prime Contractor	TSA		HTRR SRMD: SSHA, SHA, O&SHA, SSAR SSPP SAR		
Service Unit SM/Safety Engineer	Assist/ Review	Assist/ Review	Assist/ Review	Assist/ Review	
ATO SSWG	Review and Concur	Review and Concur	Review and Concur	Review and Concur	
ATO SSWG Chair	Concur (5)	Concur (5)	Approve (5)	Concur	
ATO Director of SMS	Approve (6)	Approve (6)	Approve (6)	Approve (6)	
Service Unit	Accept Risk	Accept Risk	Accept Risk	Accept Risk	
AOV				Approve Controls for Initial High Risk Hazards	

Notes:

1. The safety plan developed needs to be included in the following documents: Enterprise Architecture, preliminary Program Requirement (pPR) Section 14, Concept and Requirements Definition (CRD) Plan and the IAP.
2. SMS Manual 2.1 – Section 3.5.2, SRMDM: No Safety Risk Introduced to the NAS
3. A CSA is required if there is more than one solution alternative. If there are no alternatives, go directly to the PHA. The PHA uses the information available on the selected solution. This may be the functional requirements in the System Level Specification. In this case, the SRMD may be termed a Functional Requirements PHA.
4. PHA is performed on the selected alternative solution.
5. The ATO SSWG Chair approves the Safety Strategy included in the CRD and the PSP. The Chair concurs on all SRMDs.
6. The Director of SMS will approve SRMDs per SMS Manual.

Figure 5.1-1: Analysis Timetable

5.2 Roles and Responsibilities

This section details the roles and responsibilities of each organization involved in implementing AMS and SRM in system acquisitions. (See Appendix A, Acquisition Management Policy, in the FAST for a complete description of Roles and Responsibilities for the JRC, EC, Vice Presidents, Service Directors, Service Team, Service Team Lead, and Service Organizations.)

5.2.1 JRC Secretariat

The JRC Secretariat maintains a JRC RCC which ensures appropriate SRM documents required for all investment decision meetings have been coordinated with the Office of Safety. A representative from the SRM Office will ascertain completion of SRM documents pertaining to programs at the weekly JRC readiness review meetings.

5.2.2 AVS

AVS is the FAA organization responsible for establishing certification standards for aircraft, operators, and air carriers. AVS also approves and issues Flight Standards. AVS includes the AOV, which oversees the SMS process in ATO in accordance with FAA Order 1100.161.

AVS roles and responsibilities under SRM are:

a. Perform SRM for changes to the NAS that may impact safety risk. (The SMS requires that all hazards related to aircraft certification and flight standards associated with a change be identified and treated.)
b. Designate one ATO SSWG representative each from Flight Standards and Aircraft Certification and ensure attendance.
4. These representatives ensure that the appropriate AVS personnel review and comment on all safety analyses and plans submitted to the ATO SSWG for review in accordance with this plan.
5. At least one of the designated AVS representatives must be in attendance for the ATO SSWG to approve system safety analyses of systems that have documented safety hazards affecting the safe conduct of flight by aircraft or airmen or in which Federal Aviation Regulations are considered as controls for any hazard.

5.2.3 Service Units

For En Route and Oceanic Services, Terminal Services, Technical Operations Services, System Operations Services, and NextGen and Operations Planning Services, each Vice President has delegated responsibility to the Safety Manager and Safety Engineers to guide and support the Service Teams in preparing the safety documents and to represent the Service Unit at the ATO SSWG. Safety Managers ensure that the Vice President of their Service Unit is informed of the risks involved in a proposed change to the NAS and recommend

SRMD approval and risk acceptance in accordance with the latest version of the SMS Manual.

5.2.3.1 Service Unit Service Team

One of the roles of the Service Team is to identify and prioritize future FAA needs and technology opportunities in the service-level mission need assessment that is updated annually.

The Service Team defines the planned safety effort during the IA phase for inclusion in the plan for initial and/or Final IA and to ensure that the required safety products are prepared to support the JRC decision process. The Service Team must:

1. Provide a central point of contact to coordinate all safety analyses throughout the program's lifecycle.
2. In a safety strategy meeting with the ATO SSWG Chair, determine what safety effort is required.
3. Document the rationale in an SRMDM with ATO SSWG concurrence and approval from the Director of SMS. The Service Team must include the SRMDM rationale as part of the JRC briefing.
4. Conduct the analyses in accordance with the instructions in the AMS FAST.
5. Ensure adequate resources and trained personnel are assigned to an SRM Panel to perform and document the safety assessments and analyses.
6. When the SRMD and PSP drafts are complete and have been reviewed by the responsible Service unit organizations, submit them to the ATO SSWG for review and final concurrence.

The Service Team Lead must:

1. Submit required safety documentation to the ATO SSWG Secretariat at the scheduled date to ensure timely decisions in support of the JRC Readiness Review process.
2. Determine the level of safety analysis required, gain concurrence from line management (Safety Manager/Safety Engineer, group, office, and Director as appropriate) and submit the SRMD or SRMDM to the ATO SSWG through the Service Unit Safety Manager.
3. Coordinate the safety inputs to the JRC briefing.
4. Ensure that any requirements developed as a result of the safety analyses are included as discrete requirements in the pPR.
5. Ensure that SRM Panels assigned throughout the program's lifecycle comply with the SMS Manual and this document.
6. Verify that the mitigations (validated and verified safety requirements) are included in the system before it is implemented, in accordance with the SMS.

7. Document all decisions and assessments made in the program's SRM effort; systematically review and investigate safety-related reports on the operation or test of new systems, including air traffic incident reports and reports on failures and degraded service, to detect hazards and adverse trends.
8. Ensure that the Service Team monitors and audits the safety performance of the program after the ISD.
9. Conduct SRM for the lifecycle of the program.

5.2.3.2 IAT

The role of the IAT in implementing SRM is to determine the need for and direct performance of CSAs of the alternatives and to require development of the program's PSP.   The IAT is led by the Service Unit Safety Engineer representative to the team.

Specific responsibilities for the IAT, as facilitated by its Service Unit representative:

1. Provide a central point of contact to coordinate safety analyses.
2. Ensure that the PSP is included, at least by reference, in the ISP document.
3. Include the results of the CSA in the BCAR.

5.2.3.3 ASAG

The ASAG is a cross-organizational body that evaluates proposed changes to acquisition management policy and guidance to ensure that changes comply with the policy for AMS Change Management.   Changes to the SRMGSA are submitted to the ASAG prior to incorporating into the AMS guidance.

5.2.3.4 Office of Safety, Director of SMS

The Director of SMS has the primary responsibility to develop, implement, and coordinate the SRM process in the ATO. He or she promotes the use of system safety principles across all the FAA Service Units. The Safety Managers within the ATO and other senior safety engineers from all LOBs meet periodically to advise the Director of SMS on the status of SRM activities.

The Director of SMS must:

1. Determine the risk acceptance authority, in accordance with the SMS, for each hazard tracked in the HTS.
2. Brief the EC on safety issues upon request by the Service Team.
3. Monitor and audit system safety programs for compliance with the SMS.

5.2.3.5 Chair, ATO SSWG

The Chair will participate in the SRM process for the acquisition of systems in the AMS. The Chair must:

1. Develop, maintain, and manage the SSWG process.
2. Advocate, support, and control the SRM process for system acquisitions.
3. Advise and guide the programs and analysis teams in conducting SRM.
4. Conduct Safety Strategy meetings with the Service Team at the initiation of the system acquisition activities (e.g., start of MA, IID, etc.)
5. Approve all PSPs.
6. Provide recommendations for approval of SRMDs and acquisition related SRMDMs to the Director of SMS.
7. As needed, provide SSPR to the Director of SMS covering safety plans, assessments, reports, and analyses in accordance with this document.
8. On request, brief all JRCs on the status, conduct, and results of SRM activities of each program. Provide recommendations to the JRC on the program's continuation into the next phase based on the SRM status and progress of the program. This briefing must be coordinated with the Service Teams, Business Case Analysis Teams, and Business Case Evaluation Teams prior to the JRC and early enough for the implementation team to take remedial action.
9. Help other LOBs establish SRM plans and processes.
10. Review the SRMD and the safety assessments, analyses, reports, and plans that accompany the SRMD; provide concurrence or recommendations for changes required for concurrence within 10 working days of receipt. This concurrence is limited to verifying that the process used in the safety analysis is consistent with the process defined in this document and in the SMS Manual or other industry standard alternatives, and that the analysis has identified the known hazards and that their associated RACs are at the right level of risk.
11. Upon request, assist the Director of SMS in briefing the JRC on the results of the system safety effort (risks, mitigation strategies, and safety requirements) for each program.

5.2.3.6 ATO SSWG

The ATO SSWG promotes and guides the SRM process in the acquisition of systems in the NAS. In addition, the ATO SSWG assists the teams responsible for conducting or managing system safety programs. Appendix I contains the charter for the ATO SSWG. The ATO SSWG must:

1. Support the review and analyses of SRM documentation consistent with the planned timing of JRC decisions.
2. Recommend changes required for approval of PSPs; give recommendations for needed changes to the originating team within three weeks' receipt of the PSP.
3. Review the HTRR system to track the status of hazards and their associated controls and requirements to eliminate or control the assessed

risk throughout the lifecycle of a program; make recommendations for corrective action to the Service Teams, as appropriate.

- Review all SARs contained in the HTS and, at a minimum, review all open hazards with an initial RAC that is medium or high. While reviewing each SAR, review the validation and verification status of each safety requirement/control, including the evidence of verification, and confirm the

4. Recommend the risk acceptance authority to the Director of SMS, in accordance with SMS for each SAR tracked in the HTS; coordinate with other elements of the NAS to identify and evaluate areas in which safety implications exist (e.g., Aircraft Certification, Flight Standards, Human Factors, Security).

5. Identify, evaluate, and document lessons learned.

APPENDICES A – M

Bow-tie Model
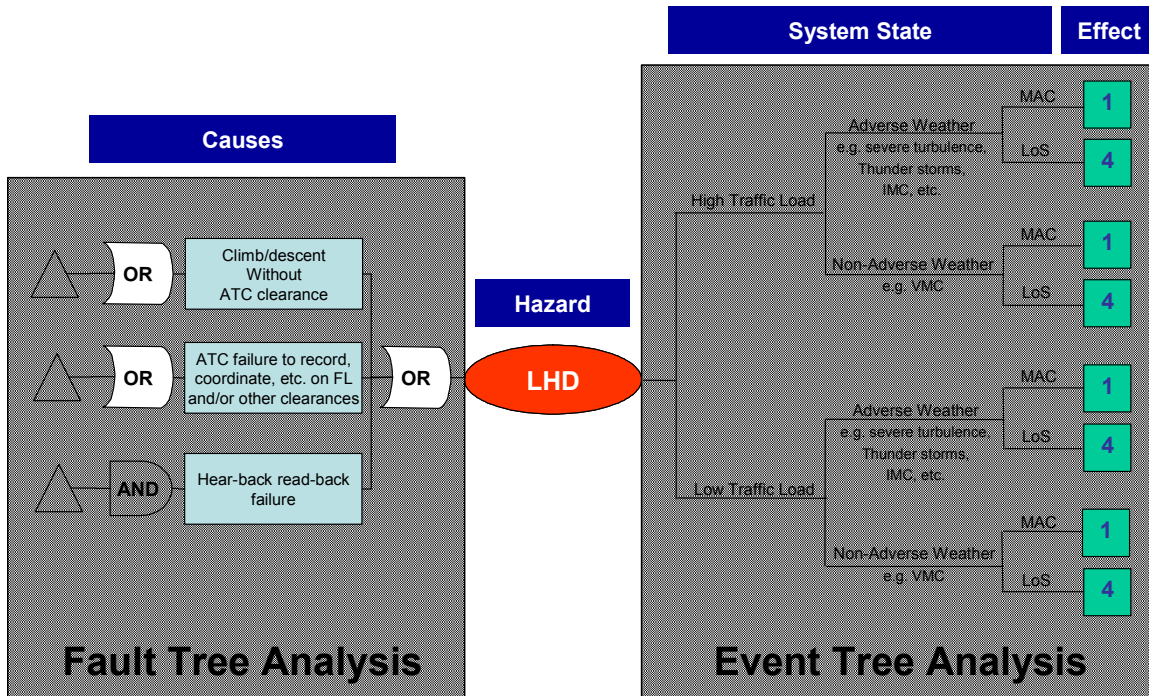
In this example, the identified hazard is a Large Height Deviation (LHD). Some of the high-level causes are identified on the left side. If this were an actual analysis, each cause would likely be broken down further into sub-causes. To the right of the hazard, the system state is identified as high traffic load or low traffic load. These system states are further broken down into adverse weather and non-adverse weather. Each one of these system states results in an effect (Mid Air Collision or Loss of Separation). The effects have then been rated for severity (in the boxes), with one representing a catastrophic event and five representing minimal. The worst credible effect in this example occurs when a LHD occurs during adverse weather conditions in either high or low traffic loads. Therefore, these sequences would be used in the safety risk analysis.

Appendix B: Operational Safety Assessment Outline

The OSA report is documented in an SRMD and contains the following:

1. Executive Summary including the findings, and the safety objectives and requirements

2. Purpose-including relevant background information.

3. Scope

4. A list of assumptions, definitions, and a description of the tools used.

5. Operational Service and Environment Description (OSED) - The OSED is a description of: the system's physical and functional characteristics, the environment's physical and functional characteristics, and air traffic services and operational procedures. It includes both air and ground elements of the system analyzed and includes the Functional Assessment. The FA can be in an Appendix to the OSA subset of the SRMD.

6. Operational Hazard Analysis (OHA) – The OHA is a qualitative severity assessment. The OHA includes tabular worksheets. An example format is shown in Appendix C of this SRMGSA.

7. Assignment of Safety Objectives and Requirements (ASOR)

8. Conclusions and Recommendations

9. References

10. List of Figures

11. List of Tables

12. Appendices for the FA, OHA and any other required information

Refer to RTCA DO-264 (Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications).

Tabular Format for OSA

Hazard No.	Hazard Description	Causes	System State	Possible Effects	Severity/ Rationale	Existing Controls and Requirements[1]	Recommended Safety Controls or Requirements	Safety Objective
See Appendix C: "Hazard Number" for the format	Refer to the model in Appendix A. Using that model, this is the hazard	Refer to the model in Appendix A. Using that model, these are the causes for the hazard	Refer to the model in Appendix A. Using that model, this is the worst case system state for the hazard to occur.	Refer to the model in Appendix A. This is the worst credible outcome if the hazard occurs in the worst case system state.	Refer to Section 3.2 for severity definitions	These are the existing controls or requirements (validated or verified), safety features, warnings, or procedures that mitigate the effects, system state or hazard occurrence.	These are the engineer's recommendations for additional controls and requirements that have the potential to mitigate the hazard but are not validated at the time of the assessment.	The OSA is not a risk assessment. The safety objective is the least likelihood to achieve at least the minimum level of acceptable risk I.e., Medium, however, a lower risk target may be identified by the analyst as desirable if cost and schedule permit
ADS-001	One engine in-operative	Fuel line crimped. Ice accretion on intake. Faulty engine control. Crew inadvertently pulls engine off line. Water in fuel cell.	Low Altitude. Low Airspeed. High-density altitude. High gross weight.	Loss of power from one engine. Power required exceeds power available. High rate of descent. Impact before single engine airspeed can be reached. Fatal injuries to occupants.	1 Catastrophic due to loss of aircraft	Two engines. Two fuel cells. Water drains. Ice Protection. Dual engine controls. Clearly marked engine control levers. Pre-flight inspection requires crew to examine fuel lines. Etc.	The height-velocity curve should be adjusted. The engine control levers shall be secured when in the 'fly' position. The crew shall have to activate a button to move out of 'fly.'	Medium or Low

Appendix D: Program Safety Plan Template

The Program Safety Plan Template is available on the ATO SSWG KSN website at

https://ksn.faa.gov/km/atos/smssrm/sswg

Contact the ATO SSWG Chair for access.

Tabular formats should be used when the information contained in the cells is brief and does not overflow onto subsequent pages. Typically tabular formats are used in the OSA, CSA, PHA, SHA, and SSHA. References in the table are to Sections or Appendices in this SRMGSA.

Tabular Format

Hazard No.	Hazard Description	Causes	System State	Existing Controls and Requirements[1]	Possible Effects	Severity/ Rationale	Likelihood/ Rationale	Current Or Initial Risk	Recommended Safety Controls or Requirements	Predicted Residual Risk
See Appendix C: "Hazard Number" for the format	Refer to the model in Appendix A. Using that model, this is the hazard	Refer to the model in Appendix A. Using that model, these are the causes for the hazard	Refer to the model in Appendix A. Using that model, this is the worst case system state for the hazard to occur.	These are the existing controls or requirements (validated or verified), safety features, warnings, or procedures that mitigate the effects, system state or hazard occurrence.	Refer to the model in Appendix A. This is the worst credible outcome if the hazard occurs in the worst case system state.	Refer to Section 3.2 for severity definitions	Refer to Section 3.2 for likelihood definitions	See definitions and guidelines in section 3.2.1	These are the engineer's recommendations for additional controls and requirements that have the potential to mitigate the hazard but are not validated at the time of the assessment.	Refer to Section 3.2.1 for definitions. \ This shows risk when existing and recommended controls or requirements are verified.
ADS-001	One engine in-operative	Fuel line crimped. Ice accretion on intake. Faulty engine control. Crew inadvertently pulls engine off line. Water in fuel cell.	Low Altitude. Low Airspeed. High-density altitude. High gross weight.	. Two engines. Two fuel cells. Water drains. Ice Protection. Dual engine controls. Clearly marked engine control levers. Pre-flight inspection requires crew to examine fuel lines. Etc.	Loss of power from one engine. Power required exceeds power available. High rate of descent. Impact before single engine airspeed can be reached. Fatal injuries to occupants	1 Catastrophic due to loss of aircraft	D Extremely remote due to redundancies	1D High	The height-velocity curve should be adjusted. The engine control levers shall be secured when in the 'fly' position. The crew shall have to activate a button to move out of 'fly.'	1E Medium

Note 1. See System Engineering Manual, Sect 4.12 for clarification of the difference between validated and verified requirements.

Appendix F: Outline of the System Safety Assessment Report

The following outline should be used as a guide for development of the SSAR. Specific guidance on the conduct of safety reviews is contained in the Safety Review SOP, posted on the ATO SSWG KSN web site.

1. Executive Summary

2. System Description

3. Summary of safety analyses conducted through the lifecycle of the program

4. Results of analysis and tests performed to verify the safety requirements (and other verification activities)

5. List of hazards (with risk) identified to date

6. SRVT

7. Results of SAR review including objective evidence of verification of controls, mitigations and requirements

8. Safety Action Records signed by the Risk Acceptance Authority

Appendix G: Safety Requirements Verification Table

Allocation: Safety Requirements Verification Table		R/O Source	V&V Status	Allocation		Planned V&V Method		Risks Controlled by SRVT		
PUI	Requirement or Objective (R/O)			AC	GND	Test	Assess	Hi	Med	Low
51.	Develop contingency procedures for specific collision hazard situations (OPEVAL 2 scenarios)	PHA		X	X	X		2	21	
52.	Develop contingency procedures for specific collision hazard situations (OPEVAL 2 scenarios)	SSHA		X			X	1	12	223
	Adequate training and certification of aircrew to ensure situational awareness, appropriate equipment usage, and information interpretation	SHA		X			X	3	11	100
	Failure/malfunction indication shall be designed to conform to appropriate standards, (e.g., Human Factors Design Standard HF-STD-001 DOT/FAA/CT-03/05, May 2003)	SHA		X	X	X			34	12
	Pilot uses "see and avoid" procedures	O&SHA		X				1	12	16
80.	Avionics certification, installation, approval process in place for OPEVAL 2	OSA	Figure	X			X	1	14	45
41.	The equipment used in OPEVAL 2 shall be designed to conform to appropriate standards, (e.g., Human Factors Design Standard HF-STD-001 DOT/FAA/CT-03/05, May 2003)	O&SHA				X	X	1	10	22

The CSA Summary Sheet template depicted on the following pages may be opened by **double clicking** on the page anywhere within the CSA Summary Sheet. The CSA Summary Sheet is the cover page for the CSA and all contents within the document. The document should be saved for use under a separate file name by selecting <u>F</u>ile and clicking on **Save Copy <u>A</u>s** and assigning a new file name.

After saving the newly named file to another directory, select <u>F</u>ile and click on **Close & Return to SRMGSA_Rev_ (current document revision).doc**. This will restore the view to the entire SRMGSA document.

Within the opened CSA document itself, the fonts, and table arrays are preset to the values of the desired CSA Summary format. Fonts and table arrays may be altered at the author's discretion for size and composition.

Following preparation and peer review, the CSA is to be transmitted electronically to the ATO SSWG for review.

Content of the sample CSA template contained herein is fictional and does not represent an actual CSA requested or required by the Federal Aviation Administration nor does it relate to existing or pending Federal Communications Commission rules or regulations.

NOTE 1: You must double click on the following CSA template to open it up all the way. See the instructions at the top of this page for how to save your own copy of it.

NOTE 2: You must have access to this template in soft copy for these instructions to be meaningful. The SRMGSA in Word format can be found at http://fast.faa.gov/toolsets/SafMgmt/indexstart.htm

CSA SUMMARY SHEET *(Double Click to Open)*	*Insert document control number here*
Chief System Safety Engineer _____	**Requesting Organization**: *Insert FAA or other requestor here*
Title/Subject: *Insert title of qualitative or quantitative Comparative Safety Assessment (CSA) here*	**Date**: *Insert preparation date and subsequent revisions and dates here (e.g. August 1, 2001, Rev. A, October 16, 2001)*

Subject Description: [preset to Body Text] *Insert subject description of Comparative Safety Assessment here*

Problem Statement: [preset to Heading 6]:

Insert a problem statement paragraph here - (e.g. "The Academy of Model Airplane Aeronautics (AMA) members want to add capabilities to their radio control (RC) aircraft models to operate on frequencies within the 49.8 MHz range presently reserved for radio control of models other than aircraft. While the frequencies of 49.830 MHz, 49.845 MHz, 49.860 MHz, 49.875 MHz, and 49.890 MHz are authorized, power output is limited to 100 Milliwatts amplitude modulated control signals and therefore is not recommended for control of model aircraft by today's restrictions. The AMA's reason for wanting to transmit and receive at 49 MHz instead of the presently authorized frequencies of 72 MHz is that baseband amplifiers are more readily available on today's market which would permit higher transmitter power to be used and would enable AMA model enthusiasts to competitively operate aircraft at greater distances. Their additional claim is that with the advent of 49 MHz digital wireless telephone products, the cost to produce the radio control transmitters and receivers is 40% less than the cost to produce the presently acceptable 72 MHz analog transmitters and receivers.

Should RC model aircraft enthusiasts be permitted to operate at 49 MHz with higher-power output transmitters with digital modulation, which could interfere with nearby 49 MHz wireless telephone communications, or conversely could such nearby telephone transmitters interfere with model aircraft operations, thus causing loss of control that could lead to hazards.)

Expand upon conditions warranting CSA in the following paragraphs [restrict to three to five total] - (e.g. Fiercer "dog-fight" and pylon competition in expanded areas of operation are attainable with higher RC transmitter power output operating at 49 MHz compared with the lower-power output of 100 Milliwatts as the Federal Communications Commission (FCC) rules now limit for 49 MHz or with RC transmitters operating at 72 MHz frequencies. The safety related question is:

    a. *With operations possible at greater distances from a digital time division multiple access RC transmitter accorded through increased power output, would there be a higher likelihood of injury or loss of aircraft resulting from potential loss of positive control of the RC model aircraft?*

The AMA deems safety for spectators, participants, and contest personnel to be of the utmost importance. Hazardous flying over the racecourse or any flying over controlled spectator areas or pits during competition is a "black flag offense." Loss of control of an aircraft can be hazardous especially for officials judging a dog-fight or pylon competition whether on or off the course.

The functional analysis performed against the analog 72 MHz RC transmitters found several spurious emissions of the control signals were possible due to poor propagation factors and interference from other 72 MHz digital-proportional and amplitude modulated RC transmitters operating in close proximity within the competition areas, which could cause loss of control of one or more RC model aircraft. The functional analysis also showed that the 72 MHz analog superhetrodyne receivers generally provided little harmonic signal rejection to cross-and inter-modulation, thus leading to possible contamination of a received signal controlling one or more axis of a given RC model aircraft operating on the course, in close proximity to another RC model aircraft operating on or at an adjacent frequency. One mitigating factor in the perturbance of the analog control signals or as a consequence of reduced received signal-to-noise is that the RC model aircraft would assume a level-flight condition, albeit under previously commanded engine power, thus possibly reducing injury to personnel within the immediate vicinity of the race course or operating area. However, such condition could lead to hazards outside of the area through loss of positive radio frequency control.

The functional analysis performed against the digital 49 MHz frequency or phase modulated digital time division multiple access RC transmitters at 100 milliwatts output power revealed fewer spurious emissions of the control signals however, when the power output was increased to 3 watts, some spectral splatter was observed due to poor construction of the specimen RC transmitter. It is likely that such splatter condition could be diminished with a better-designed and manufactured RC transmitter. Regardless, it is unlikely, that several compatible digital 49 MHz receivers all operating on adjacent frequencies within a group or cluster of

Appendix I: ATO System Safety Working Group Charter

1. Purpose: To establish a technically qualified advisory group sponsored by the ATO Office of Safety Safety Risk Management (SRM) Office made up of FAA System Safety professionals. The ATO System Safety Working Group's (ATO SSWG) purpose is to provide system acquisition guidance for conducting SRM in accordance with the SMS Manual and the SRMGSA. The SRMGSA provides more detailed safety guidance for system acquisitions in accordance with the SMS Manual. The ATO SSWG also provides safety program status (in consultation with the Service Unit) and recommendations to the Director of SMS on safety plans and assessments where those may be required.

2. Scope: The ATO SSWG is responsible for advising the Director of SMS regarding reviews of Program Safety Plans and Safety Risk Management Documents (SRMDs), including safety analyses as appropriate to the nature of the proposed change. In addition, the ATO SSWG advises the Operational Service Units, Lines of Business (LOBs), and Service Teams, in establishing system safety and SRM programs for system acquisitions and changes to legacy systems.

The ATO SSWG will function as an element of program management to monitor the accomplishment of the following system safety tasks pertaining to system acquisitions:

    c. Validation of system safety program plans;
    d. Identification of system safety requirements;
    e. Organization and control of those interfacing FAA efforts that are directed toward the mitigation or control of system hazards;
    f. Coordination with other program management elements; (e.g., requirements management, IA process)
    g. Analysis and evaluation of candidate system safety programs to provide timely and effective recommendations for improving program effectiveness.
    h. Coordination and integration of ground-based and airborne hazard analysis, including review of safety requirements validation and verification.

3. Authorizations: The ATO SSWG is chartered by ATO Office of Safety in accordance with the ATO's implementation of the ATO SMS Manual. It is organized to comply with the FAA AMS, the SRMGSA and the SMS Manual.

4. References:

    1. ATO SMS Manual (Latest Revision)
    2. Safety Risk Management Guidance for Acquisitions (SRMGSA), (Latest Revision). See http://fast.faa.gov.
    3. FAA Acquisition Management System (Latest Revision). See http://fast.faa.gov/.
    4. Joint Resources Council (JRC) Readiness Criteria and Checklist (Latest Revision).
    5. FAA Hazard Tracking Systems for Acquisitions and Operations. (Contact ATO SSWG Secretariat for information and/or access.)
    6. Office of Management and Budget (OMB) Exhibit 300 and FAA Attachments (Program Requirements, BCAR, Implementation Strategy and Planning (ISP) document)
    7. FAA Order 1100.161 Air Traffic Oversight (Latest Revision)
    8. ATO Order JO 1000.37 Air Traffic Organization Safety Management System (Latest Revision)

5. **Tasks:** The ATO SSWG is responsible to the Director of SMS for the following:

   a. Recommending changes required for approval of Program Safety Plans (PSPs).
   b. Providing recommendations for needed changes will be given to the originating team within three weeks of receipt of the PSP.
   c. Maintaining a HTRR system to track the status of hazards and their associated controls and requirements to eliminate or control the assessed risk throughout the lifecycle of a program. The ATO SSWG will make recommendations for corrective action to the Service Teams, as appropriate.
   d. Reviewing all Safety Action Records (SARs) contained in the HTS and, at a minimum, reviewing all open hazards with an initial RAC that is medium or high. During review of each SAR, the ATO SSWG will review the validation and verification status of each of the safety requirements/controls, including the evidence of verification, and will confirm the SAR status and RAC in accordance with the SRMGSA
   e. Recommending the risk acceptance authority in accordance with SMS for each SAR that is tracked in the Hazard Tracking System (HTS).
   f. Coordinating with other elements of the NAS to identify and evaluate areas in which safety implications exist (e.g., Aircraft Certification, Flight Standards, Human Factors, EEOSH Services, Security).
   g. Identifying, evaluating and documenting lessons learned.

6. **Document Approval and Risk Acceptance Process**

Upon receipt of the ATO SSWG's recommendations, the Director of SMS roles and responsibilities are such that:

   a. The Director of SMS is the approval authority for identified SRMDs where required by the SMS Manual.
   b. The Director of SMS shall ensure that the risk acceptance authority for safety analyses is in accordance with SMS.
   c. The Director of SMS upon request will brief the ATO EC and FAA Joint Resources Council (JRC), regarding the safety risks, mitigation strategies, and safety requirements for a program.

Figure K-1 shows the process flow for a SRMD which contains the safety analyses required under the AMS. It defines the responsibility for the Service Unit, ATO SSWG, Chair, Director of SMS, and the ATO SSWG Manager.

- The Service Team shall submit the SRMD to the Service Unit Safety Manager for review and concurrence.
- The Service Unit Safety Manager or Designee shall submit the SRMD to the ATO SSWG.
- The ATO SSWG reviews the SRMD for compliance with the SMS and SRMGSA.
- Results of the review are fed back to the Service Unit for changes if required.
- After needed changes are made and the review is complete, the Chair concurs and recommends the approval to the Director of SMS.
- The Director of SMS approves the SRMD and determines the risk acceptance authority in accordance with the SMS Manual.
- The ATO SSWG Secretariat prepares a transmittal memorandum (SSPR) for the Director of SMS to send the SRMD to the Service Unit for risk acceptance.

- Service Unit signs the SRMD and accepts the risk associated with the identified hazards and transmits the signed original to the ATO SSWG Secretariat to retain in the Safety Case File.
- SRM Office verifies at the JRC Readiness Review meeting completion/approval of required SRM documents.
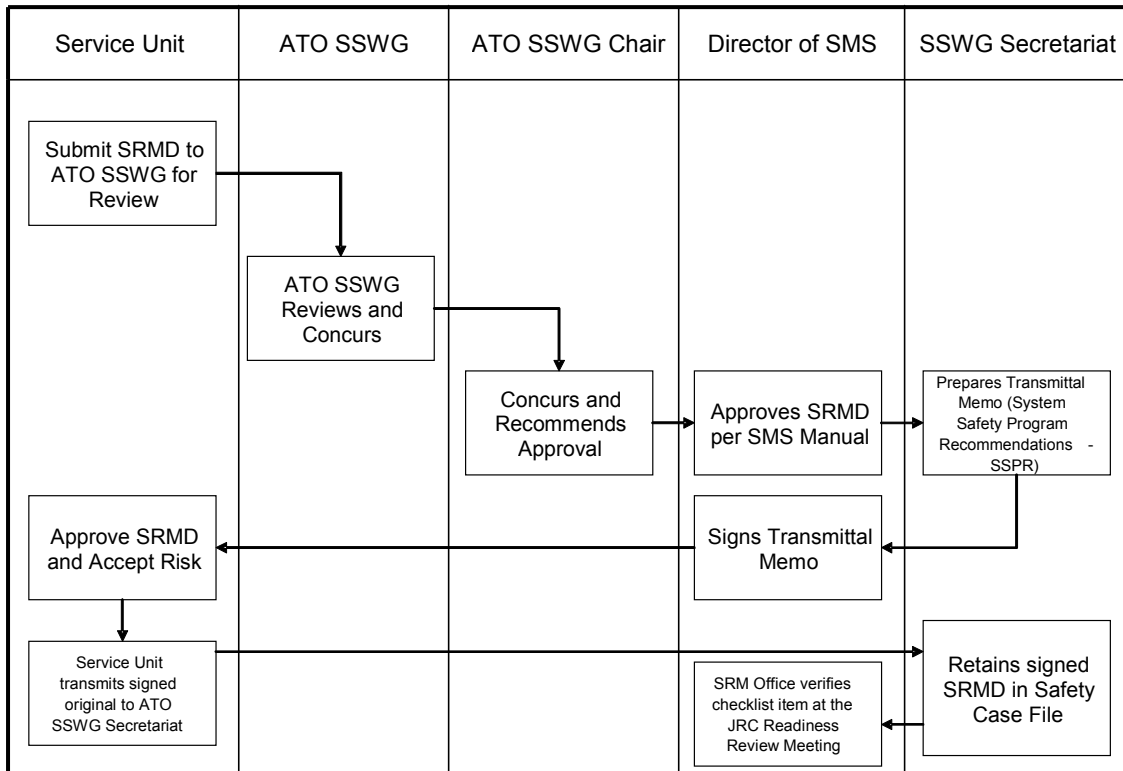

Figure I-1: ATO SSWG APPROVAL and RISK ACCEPTANCE PROCESS

Note: This flow chart is generic for an SRMD (with safety analysis e.g. OSA, CSA, PHA, SSHA, SHA, O&SHA, SSAR) that are going through the SRM process. The ISR checklist begins early in the lifecycle and forms a part of the JRC Readiness Checklist at each decision point throughout the lifecycle (i.e., IARD, IID, FID, ISD).

7. ATO SSWG Operation

a. *Chair*. The ATO SSWG is chaired by a Safety Engineer from the SRM Office

b. *Membership*. The ATO SSWG is composed of representatives from the various ATO Service Units, LOBs, and Service Teams.

b.1 Principal members are:

ATO Service Unit Safety Managers (from En Route, Oceanic, Terminal, Technical Operations, System Operations, and NextGen and Operations Planning)

ATO Service Unit Safety Engineers (from En Route and Oceanic, Terminal, Technical Operations, System Operations, and NextGen and Operations Planning)

Principal members:
(1) Attend and participate in the ATO SSWG meetings.
(2) Review and comment on the plans and analyses that come to the ATO SSWG to ensure that all known hazards have been identified and that the risk level associated with the hazard is at the right level;
(3) Ensure that the documentation is consistent with the safety process defined in the SRMGSA; and
(4) Provide comments and recommend changes as required for approval of the system safety PSP and SRMD.

b.2 Members-at-Large will be appointed by the Chair and approved by the Director of SMS from the following organizations. They will participate and provide input and advice based on their expertise in the subject matter under review, and may be required to concur on the document.

AIR	Aircraft Certification Service
AFS	Flight Standards
AST	Office of Commercial Space
ATO-W	EEOSH Services
ATO-P	Human Factors

b.3 Advisory members will be invited from other organizations as appropriate:
Advisory members will be invited to attend meetings when their expertise, opinions, or comments are required or solicited.

b.4 Secretariat
The ATO SSWG Secretariat will be provided by ATO Office of Safety.

b.5 Changes in membership will be as required to fulfill the purpose of the ATO SSWG. Such changes will be subject to approval of the Chair.

c. Quorum. In order for the ATO SSWG to review and concur on a document
 or report, it must have a quorum. A quorum is defined as the following being present:

1. ATO SSWG Chair;
2. A designated principle representative of the affected Service Unit (the Safety Manager or Safety Engineer);
3. A designated representative of the program sponsoring or conducting the SRMD under review.
4. A designated representative from Aircraft Certification (AIR) as required.
5. A designated representative from Flight Standards (AFS) as required.

d. Attendance. Anyone within the ATO may attend ATO SSWG meetings and anyone may propose a topic of discussion. All recommendations made by the ATO SSWG regarding review and concurrence of SRMDs will be made on a consensus basis. Consensus in this context means all members present can accept the resulting decision. Non-concurrence by a member will be documented in the SRMD.

e. Meetings. ATO SSWG meetings will be held monthly on the 2nd Tuesday of each month. Notification of the meeting time, location and agenda will be posted on the ATO SSWG KSN Website 2 weeks prior to each meeting. A meeting may be cancelled if there is no business in the queue. Special meetings may be scheduled when required by the Service Team to support program decisions. Principal members will attend all meetings. Members-at-Large and other members will attend meetings at the invitation of the Chair when their specialized expertise is required. Meetings may be conducted by teleconference in those cases where time does not allow the ATO SSWG to meet in person.

f. Administration.

1. The ATO SSWG Chair will establish the agenda for scheduled meetings no later than two weeks prior to the meeting;
2. Service Team representative briefs the SSWG chair and Secretariat on the analysis/document the Service Team is submitting to the SSWG prior to establishing the agenda and identify participants required for the meeting.
3. Documentation for review by the ATO SSWG members will be posted on the KSN website 10 working days prior to the meeting. The KSN site is https://ksn.faa.gov/km/atos/smssrm/sswg. The site administrator (ATO SSWG Secretariat) will advise (by email) those members who are to attend and provide ID and passwords for access to each member.
4. The ATO SSWG will accept proposed agenda items submitted by any principal or advisory member of the working group;
5. The ATO SSWG minutes will be prepared for each meeting. A summary of action items, action agencies, and suspense dates will be prepared before the end of the meeting. Formal minutes of each meeting will be prepared and posted on the KSN site by the ATO SSWG Secretariat;
6. The ATO SSWG Secretariat will maintain a case file for each program/project documentation (e.g., SRMDs, PSPs, meeting minutes, other relevant correspondence and notes).
7. The ATO SSWG recommendations submitted to the Service Team will include minority opinions when appropriate;
8. The ATO SSWG will review all items from previous meetings, as required, to determine that an action is closed or adequate progress is being made;
9. The ATO SSWG will review this charter at least annually, and update or modify it as required.

Appendix J: Data Item Descriptions (DIDs) Templates

Contents:

DATA ITEM DESCRIPTION	
1. TITLE **Preliminary Hazard Analysis**	2. IDENTIFICATION NUMBER FAA-DI-SAFT-101

3. DESCRIPTION/PURPOSE

3.1 THE PRELIMINARY HAZARD ANALYSIS (PHA) is an initial effort in hazard analysis during the system design phase and the programming and requirements development phase for acquisition. It may also be used on an operational system for the initial examination of the state of safety. The PHA is primarily used to perform an initial risk assessment and to develop safety-related requirements and specifications early in the acquisition. The PHA is used to both identify new requirements and to support the validation and verification of existing requirements.

4. APPROVAL DATE (YYYY/MM/DD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) **ATO-S SAFETY RISK MANAGEMENT OFFICE (AJS-2)**

6. APPLICATION/INTERRELATIONSHIP
6.1 This Data Item Description (DID) contains the format and content preparation instructions for the PHA.
7. PREPARATION INSTRUCTIONS
7.1 Reference documents. The applicable issue of the documents cited herein, including their approval dates and dates of any applicable amendments, notices, and revisions shall be as specified in the contract and in accordance with the SRMGSA in the AMS FAST Toolset.

7.2 Format. The PHA format shall be "contractor selected" from either the narrative or tabular styles, as defined in the SRMGSA, Appendix E. Unless the effective presentation would be degraded, the initially selected format must be used for all subsequent submissions.

7.3 Content. The PHA is performed early in the lifecycle of a system, providing important inputs to the development of requirements in the early phases of system development. In the case of an operational system, it aids in the early determination of risk and the need for additional safety requirements for operational hazards. The output of the PHA will be used to develop system safety requirements and to assist in preparing performance and design specifications. In addition, the PHA is a basic hazard analysis that establishes the framework for follow-on hazard analyses that may be performed.

The PHA shall contain the items shown in the block 7.3.1 through 7.3.12 and be in accordance with the SRMGSA. In addition, each hazard identified shall be listed in either narrative or tabular worksheets (see SRMGSA, Appendix E) that contain, at a minimum, the information described in 7.3.1 through 7.3.11, which shall be included for each identified hazard:

7.3.1 Hazard Number: The hazard identifying numbers will be used to track hazards through validation and verification process to closure. Unique identifying numbers shall be created and marked for individual hazards, or number sequences created for clustered or hazard subsets, and be in accordance with the SRMGSA, Appendix E.

7.3.2 Hazard Description: A complete statement describing the hazard. The Safety Management System Manual, defines a hazard as "… any real or potential condition that can cause injury, illness, or death to people; damage to, or loss of, a system (hardware or software), equipment, or property; and/or damage to the environment." A hazard is a condition that is a prerequisite to an accident or incident.

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

7.3.4 <u>System State</u>: An expression of the various conditions, characterized by quantities or qualities, in which a system can exist. System state is described for each individual hazard associated with the system (e.g., adverse weather and lighting conditions, such as day, dusk, and night). The system state will also include the activity under which the harm may occur (e.g., storage, shipping, installation, testing, maintenance, replacement, decommissioning, or phase of flight, such as en route or taxiing). At a minimum, each hazard must be evaluated for risk in the worst credible system state. Other less critical system states may be evaluated if time permits, but the worst credible system state shall be considered for all hazards at a minimum. A "worst credible" system state assumes the most dangerous (supported by the facts) conditions under which the hazard is postulated to occur. System state shall be in accordance with the SRMGSA, Section 4.0.

7.3.5 <u>Possible Effect</u>: The effect is a description of the potential outcome or harm of the hazard if it occurs in the defined system state.

7.3.6 <u>Severity / Rationale</u>: The measure of how bad the results of an event are predicted to be. Severity is determined by the worst credible outcome.. Less severe effects may be considered analytically in addition to this, but at a minimum, the most severe effects are considered. Do not consider likelihood when determining severity. Determination of severity is independent of likelihood. In additional, to identifying the severity classifications from Table 4.1 Of the SMS Manual, Severity Definitions, and the Rationale for arriving at a specific severity definition must also be included. Refer to the SRMGSA, Section 4.0, for additional information on how to determine risk.

7.3.7 <u>Existing Safety Requirements</u>: The existing safeguards, safety features, protective devices, warnings, training, and procedures that control or eliminate risk. An existing safety requirement is a requirement that exist currently in the FAA (e.g., controls that were previously defined in prior analyses).

7.3.8 <u>Likelihood / Rationale</u>: Likelihood is an expression of how often an event is expected to occur. Severity must be considered in the determination of likelihood. Likelihood is determined by how often the resulting harm can be expected to occur at the worst credible severity. When determining likelihood, the worst credible system states will usually determine the worst credible severity. In additional, to identifying the likelihood classifications from Table 4.3 Of the SMS Manual, <u>Likelihood Definitions</u>, and the Rationale for arriving at a specific likelihood definition must also be included. Refer to the SRMGSA, Section 4.0, for additional information on how to determine risk.

7.3.9 <u>Current Risk / Initial Risk:</u>

Initial. The composite of the severity and likelihood of a hazard considering only verified controls and documented assumptions for a given system state. It describes the risk at the preliminary or beginning stage of a proposed change, program or assessment. Initial risk is determined by factoring both verified controls and assumptions into the system state. When assumptions are made, they must be documented as recommended controls. Once the initial risk is established, it is not changed.

Current. Current risk is the predicted severity and likelihood of a hazard at the current time. When determining current risk, both validated controls and verified controls are factored into the risk assessment. Current risk may change based on the actions taken by the decision-maker that relate to the validation and/or verification of the controls associated with a hazard.

7.3.10 <u>Recommended Safety Requirements:</u> The suggested mitigations or controls that have the potential to mitigate a hazard or risk but have not yet been validated or verified as part of the system or its requirements.

7.3.11 <u>Predicted Residual Risk:</u> Predicted residual risk is the term used until the safety analysis is complete and all safety requirements have been verified. Predicted residual risk is based on the assumption that all safety requirements will be validated and verified.

7.3.12 <u>Safety Risk Management Document</u>: The results of the analysis must be prepared into an SRMD, in accordance with the latest version of the Safety Management System Manual.

DATA ITEM DESCRIPTION	
1. TITLE **System Safety Program Plan**	**2. IDENTIFICATION NUMBER** FAA-DI-SAFT-102

3. DESCRIPTION/PURPOSE

3.1 The Contractor shall detail in the System Safety Program Plan (SSPP) the Contractor's program scope, safety organization, program milestones, requirements and criteria, hazard analyses, safety data, safety verification, audit program, training, accident/incident reporting, and interfaces.

4. APPROVAL DATE (YYYY/MM/DD)	**5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)** ATO-S Safety Risk Management Office (AJS-2)

6. APPLICATION/INTERRELATIONSHIP
6.1 This Data Item Description (DID) contains the format and content preparation instructions for the SSPP.

7. PREPARATION INSTRUCTIONS

7.1 <u>Reference documents</u>. The applicable issue of the documents cited herein, including their approval dates and dates of any applicable amendments, notices, and revisions, shall be as specified in the contract and in accordance with the SRMGSA in the AMS FAST Toolset.

7.2 <u>Format</u>. The SSPP format shall be "contractor selected." Unless the effective presentation would be degraded, the initially selected format must be used for all subsequent submissions.

7.3 <u>Content</u>. The SSPP includes details of those methods the contractor uses to implement each system safety task called for in the Government provided PSP, the Statement of Work, and those safety-related documents listed in the contract for compliance. Examples of safety-related documents include Occupational Safety and Health Administration (OSHA) regulations, DO-264 Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications, DO-278 Guidelines for Communications, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance, DO-178B Software Considerations in Airborne Systems and Equipment Certification, and other national standards, such as the National Fire Protection Association (NFPA). The SSPP lists all requirements and activities required to satisfy the system safety program objectives, including all appropriate, related tasks. A complete breakdown of system safety tasks, subtasks, and resource allocations of each program element through the term of the contract is also included. A baseline plan is required at the beginning of the first contractual phase (e.g., Demonstration and Validation or Full-Scale Development) and is updated at the beginning of each subsequent phase (e.g., Production) to describe the tasks and responsibilities for the follow-on phase.

The SSPP shall contain the following items:
7.3.1 <u>Program Scope</u>: The plan shall include a systematic, detailed description of the scope and magnitude of the overall SSPP and its tasks. This includes a breakdown of the project by organizational component, safety tasks, subtasks, events, and responsibilities of each organizational element, including resource allocations and the contractor's estimate of the level of effort necessary to effectively accomplish the contractual task.

7.3.2 <u>System Safety Organization</u>: Detail the System Safety Organization, including the following information:

- ♦ The system safety organization or function as it relates to the program organization
- ♦ Responsibility and authority of all personnel with significant safety interfaces
- ♦ The staffing plan of the system safety organization for the duration of the contract

- ♦ The procedures by which the contractor will integrate and coordinate the system safety efforts

- ♦ The process by which contractor management decisions will be made
- ♦ Who/Organization that does the work
- ♦ Organization that approves the work internally
- ♦ Organization that receives the work
- ♦ How the contractor will interface with the Service Team and FAA ATO System Safety Working Group (SSWG)

7.3.3 Program Milestones: Briefly describe the safety tasks and products. Include a program schedule (e.g., Gantt chart) of the safety tasks, including start and completion dates, reports, design reviews, and estimated staff loading.

7.3.3.1 Work Products: Describe work products (e.g., Preliminary Hazard Analysis, Subsystem Hazard Analysis, System Hazard Analysis, Operating and Support Hazard Analysis).

7.3.4 Requirements and Criteria: Describe the Safety Performance Requirements (performance requirements can be stated using, e.g., qualitative values, accident risk values, or standardized values); Safety Design Requirements (the program team should establish specific safety design requirements for the overall system) and required documentation (include description of risk assessment procedures (types of analyses to be performed) and safety precedence (the method of controlling specific unacceptable hazards); and in accordance with the NAS SEM, Section 4.3.

7.3.5 Hazard Analyses: Describe the specific analyses to be performed during the program. The analysis techniques and formats should be qualitative or quantitative to identify risks, their hazards and effects, hazard elimination, or risk reduction requirements, and how these requirements are to be met, in accordance with the SRMGSA.

7.3.6 Safety Data: Provide a list of system safety tasks, contract data requirements list (CDRL) having safety significance, and the requirement for a contractor system safety data file. The data in the file is not deliverable but is to be made available for the procuring activity's review on request.

7.3.7 Safety Verification: Describe the safety verification test and/or assessment program to be used to demonstrate the safety verification process, in accordance with SEM, Section 4.12.

7.3.8 Audit Program: Describe the techniques and procedures to be used for the audit program.

7.3.9 Training: Once the hazards related to training have been identified, describe the procedures to be applied in training operator, maintenance, and test personnel.

7.3.10 Accident/Incident Reporting: Describe the details and timing of the notification process for the program and the method of ensuring that the incidents/accidents are translated to hazards. Once the hazards are identified, they must be incorporated into a hazard tracking system.

7.3.11 Interfaces: Describe the requirements used to coordinate all the different interfaces of the contract, in accordance with SEM, Section 4.7.

MM/DD/YYYY	Previous editions are obsolete	Page 2 of 2

DATA ITEM DESCRIPTION	

1. TITLE	2. IDENTIFICATION NUMBER
Sub-System Hazard Analysis	FAA-DI-SAFT-103

3. DESCRIPTION/PURPOSE

3.1 THE SUB-SYSTEM HAZARD ANALYSIS (SSHA) is performed if a system under development contains subsystems or components that, when integrated, function together in a system. The Contractor shall examine each subsystem or component and identify hazards associated with normal or abnormal operations and determine how operation or failure of components or any other anomaly adversely affects the overall safety of the system. The SSHA should identify existing and recommended actions using the system safety precedence to determine how to eliminate or reduce the risk of identified hazards. The SSHA is used to both identify new requirements and to support the validation and verification of existing requirements.

4. APPROVAL DATE (YYYY/MM/DD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)
	ATO-S Safety Risk Management Office (AJS-2)

6. APPLICATION/INTERRELATIONSHIP
6.1 This Data Item Description (DID) contains the format and content preparation instructions for the SSHA.

7. PREPARATION INSTRUCTIONS
7.1 Reference documents. The applicable issue of the documents cited herein, including their approval dates and dates of any applicable amendments, notices, and revisions shall be as specified in the contract and in accordance with the SRMGSA in the AMS FAST Toolset.

7.2 Format. The (SSHA format shall be "contractor selected" from either the narrative or tabular styles, as defined in the SRMGSA, Appendix E. Unless the effective presentation would be degraded, the initially selected format must be used for all subsequent submissions.

7.3 Content. The SSHA is performed early in the lifecycle of a system, providing important inputs to the development of requirements in the early phases of system development. In the case of an operational system, it aids in the early determination of risk and the need for additional safety requirements for operational hazards. The output of the SSHA will be used to develop system safety requirements and to assist in preparing performance and design specifications. In addition, the SSHA is a basic hazard analysis that establishes the framework for follow-on hazard analyses that may be performed.

The SSHA shall contain the items shown in the block 7.3.1 through 7.3.11 and be in accordance with the SRMGSA. In addition, each hazard identified shall be listed in either narrative or tabular worksheets (see SRMGSA, Appendix E) that contain, at a minimum, the information described in 7.3.1 through 7.3.11, which shall be included for each identified hazard:

7.3.1 Hazard Number: The hazard identifying numbers will be used to track hazards through validation and verification process to closure. Unique identifying numbers shall be created and marked for individual hazards, or number sequences created for clustered or hazard subsets, and be in accordance with the SRMGSA, Appendix E.

7.3.2 Hazard Description: A complete statement describing the hazard. The Safety Management System Manual, defines a hazard as "… any real or potential condition that can cause injury, illness, or death to people; damage to, or loss of, a system (hardware or software), equipment, or property; and/or damage to the environment." A hazard is a condition that is a prerequisite to an accident or incident.

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

7.3.4 <u>System State</u>: An expression of the various conditions, characterized by quantities or qualities, in which a system can exist. System state is described for each individual hazard associated with the system (e.g., adverse weather and lighting conditions, such as day, dusk, and night). The system state will also include the activity under which the harm may occur (e.g., storage, shipping, installation, testing, maintenance, replacement, decommissioning, or phase of flight, such as en route or taxiing). At a minimum, each hazard must be evaluated for risk in the worst credible system state. Other less critical system states may be evaluated if time permits, but the worst credible system state shall be considered for all hazards at a minimum. A "worst credible" system state assumes the most dangerous (supported by the facts) conditions under which the hazard is postulated to occur. System state shall be in accordance with the SRMGSA, Section 4.0.

7.3.5 <u>Possible Effect</u>: The effect is a description of the potential outcome or harm of the hazard if it occurs in the defined system state.

7.3.6 <u>Severity / Rationale</u>: Severity is determined by the worst credible potential outcome. Less severe effects may be considered analytically in addition to this, but at a minimum, the most severe effects are considered. Do not consider likelihood when determining severity. Determination of severity is independent of likelihood. In additional, to identifying the severity classifications from Table 4.1 Of the SMS Manual, <u>Severity Definitions</u>, and the Rationale for arriving at a specific severity definition must also be included. Refer to the SRMGSA, Section 4.0, for additional information on how to determine risk.

7.3.7 <u>Existing Safety Requirements</u>: The existing safeguards, safety features, protective devices, warnings, training, and procedures that control or eliminate risk. An existing safety requirement is a requirement that exist currently in the FAA (e.g., controls that were previously defined in prior analyses).

7.3.8 <u>Likelihood / Rationale</u>: Likelihood is an expression of how often an event is expected to occur. Severity must be considered in the determination of likelihood. Likelihood is determined by how often the resulting harm can be expected to occur at the worst credible severity. When determining likelihood, the worst credible system states will usually determine the worst credible severity. In additional, to identifying the likelihood classifications from Table 4.3 Of the SMS Manual, <u>Likelihood Definitions</u>, and the Rationale for arriving at a specific likelihood definition must also be included. Refer to the SRMGSA, Section 4.0, for additional information on how to determine risk.

7.3.9 <u>Current Risk / Initial Risk:</u>

Initial. The composite of the severity and likelihood of a hazard considering only verified controls and documented assumptions for a given system state. It describes the risk at the preliminary or beginning stage of a proposed change, program or assessment. Initial risk is determined by factoring both verified controls and assumptions into the system state. When assumptions are made, they must be documented as recommended controls. Once the initial risk is established, it is not changed.

Current. Current risk is the predicted severity and likelihood of a hazard at the current time. When determining current risk, both validated controls and verified controls are factored into the risk assessment. Current risk may change based on the actions taken by the decision-maker that relate to the validation and/or verification of the controls associated with a hazard.

7.3.10 <u>Recommended Safety Requirements:</u> The suggested mitigations or controls that have the potential to mitigate a hazard or risk but have not yet been validated or verified as part of the system or its requirements.

7.3.11 <u>Predicted Residual Risk:</u> Predicted residual risk is the term used until the safety analysis is complete and all safety requirements have been verified. Predicted residual risk is based on the assumption that all safety requirements will be validated and verified.

7.3.12 <u>Safety Risk Management Document</u>: The results of the analysis must be prepared into an SRMD, in accordance with the latest version of the Safety Management System Manual.

DATA ITEM DESCRIPTION	
1. TITLE **System Hazard Analysis**	2. IDENTIFICATION NUMBER FAA-DI-SAFT-104

3. DESCRIPTION/PURPOSE
3.1 THE SHA is a safety risk assessment of a system that analyzes the interfaces of a system with other systems, as well as the interfaces between the subsystems of the system under study. The contractor-performed SSHA serves as input to the SHA. 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. The SHA is used to both identify new requirements and to support the validation and verification of existing requirements.

4. APPROVAL DATE (YYYY/MM/DD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) ATO-S Safety Risk Management Office (AJS-2)

6. APPLICATION/INTERRELATIONSHIP
6.1 This Data Item Description (DID) contains the format and content preparation instructions for the SHA.

7. PREPARATION INSTRUCTIONS
7.1 Reference documents. The applicable issue of the documents cited herein, including their approval dates and dates of any applicable amendments, notices, and revisions shall be as specified in the contract and in accordance with the SRMGSA in the AMS FAST Toolset. 7.2 Format. The SHA format shall be "contractor selected" from either the narrative or tabular styles, as defined in the SRMGSA, Appendix E. Unless the effective presentation would be degraded, the initially selected format must be used for all subsequent submissions. 7.3 Content. The SHA is performed early in the lifecycle of a system, providing important inputs to the development of requirements in the early phases of system development. In the case of an operational system, it aids in the early determination of risk and the need for additional safety requirements for operational hazards. The output of the SHA will be used to develop system safety requirements and to assist in preparing performance and design specifications. In addition, the SHA is a basic hazard analysis that establishes the framework for follow-on hazard analyses that may be performed. The SHA shall contain the items shown in the block 7.3.1 through 7.3.11 and be in accordance with the SRMGSA. In addition, each hazard identified shall be listed in either narrative or tabular worksheets (see SRMGSA, Appendix E) that contain, at a minimum, the information described in 7.3.1 through 7.3.11, which shall be included for each identified hazard: 7.3.1 Hazard Number: The hazard identifying numbers will be used to track hazards through validation and verification process to closure. Unique identifying numbers shall be created and marked for individual hazards, or number sequences created for clustered or hazard subsets, and be in accordance with the SRMGSA, Appendix E. 7.3.2 Hazard Description: A complete statement describing the hazard. The Safety Management System Manual, defines a hazard as "… any real or potential condition that can cause injury, illness, or death to people; damage to, or loss of, a system (hardware or software), equipment, or property; and/or damage to the environment." A hazard is a condition that is a prerequisite to an accident or incident. 7.3.3 Cause(s): Events that, result in a hazard or failure. Causes can occur by themselves or in combinations.

7.3.4 <u>System State</u>: An expression of the various conditions, characterized by quantities or qualities, in which a system can exist. System state is described for each individual hazard associated with the system (e.g., adverse weather and lighting conditions, such as day, dusk, and night). The system state will also include the activity under which the harm may occur (e.g., storage, shipping, installation, testing, maintenance, replacement, decommissioning, or phase of flight, such as en route or taxiing). At a minimum, each hazard must be evaluated for risk in the worst credible system state. Other less critical system states may be evaluated if time permits, but the worst credible system state shall be considered for all hazards at a minimum. A "worst credible" system state assumes the most dangerous (supported by the facts) conditions under which the hazard is postulated to occur. System state shall be in accordance with the SRMGSA, Section 4.0.

7.3.5 <u>Possible Effect</u>: The effect is a description of the potential outcome or harm of the hazard if it occurs in the defined system state.

7.3.6 <u>Severity / Rationale</u>: Severity is determined by the worst credible potential outcome. Less severe effects may be considered analytically in addition to this, but at a minimum, the most severe effects are considered. Do not consider likelihood when determining severity. Determination of severity is independent of likelihood. In additional, to identifying the severity classifications from Table 4.1 Of the SMS Manual, <u>Severity Definitions</u>, and the Rationale for arriving at a specific severity definition must also be included. Refer to the SRMGSA, Section 4.0, for additional information on how to determine risk.

7.3.7 <u>Existing Safety Requirements</u>: The existing safeguards, safety features, protective devices, warnings, training, and procedures that control or eliminate risk. An existing safety requirement is a requirement that exist currently in the FAA (e.g., controls that were previously defined in prior analyses).

7.3.8 <u>Likelihood / Rationale</u>: Likelihood is an expression of how often an event is expected to occur. Severity must be considered in the determination of likelihood. Likelihood is determined by how often the resulting harm can be expected to occur at the worst credible severity. When determining likelihood, the worst credible system states will usually determine the worst credible severity. In additional, to identifying the likelihood classifications from Table 4.3 Of the SMS Manual, <u>Likelihood Definitions</u>, and the Rationale for arriving at a specific likelihood definition must also be included. Refer to the SRMGSA, Section 4.0, for additional information on how to determine risk.

7.3.9 <u>Current Risk / Initial Risk:</u>

Initial. The composite of the severity and likelihood of a hazard considering only verified controls and documented assumptions for a given system state. It describes the risk at the preliminary or beginning stage of a proposed change, program or assessment. Initial risk is determined by factoring both verified controls and assumptions into the system state. When assumptions are made, they must be documented as recommended controls. Once the initial risk is established, it is not changed.

Current. Current risk is the predicted severity and likelihood of a hazard at the current time. When determining current risk, both validated controls and verified controls are factored into the risk assessment. Current risk may change based on the actions taken by the decision-maker that relate to the validation and/or verification of the controls associated with a hazard.

7.3.10 <u>Recommended Safety Requirements:</u> The suggested mitigations or controls that have the potential to mitigate a hazard or risk but have not yet been validated or verified as part of the system or its requirements.

7.3.11 <u>Predicted Residual Risk:</u> Predicted residual risk is the term used until the safety analysis is complete and all safety requirements have been verified. Predicted residual risk is based on the assumption that all safety requirements will be validated and verified.

7.3.12 <u>Safety Risk Management Document</u>: The results of the analysis must be prepared into an SRMD, in accordance with the latest version of the FAA's Safety Management System Manual.

DATA ITEM DESCRIPTION	
1. TITLE	2. IDENTIFICATION NUMBER
Operating & Support Hazard Analysis	FAA-DI-SAFT-105

3. DESCRIPTION/PURPOSE

3.1 THE OPERATING & SUPPORT HAZARD ANALYSIS (O&SHA) is performed by the Contractor primarily to identify and evaluate hazards associated with the interactions between humans and equipment/systems. These interactions include all operations conducted throughout the lifecycle of the system. 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 ensure that operation and maintenance manuals properly address safety and health requirements. The O&SHA is used to both identify new requirements and to support the validation and verification of existing requirements.

4. APPROVAL DATE (YYYY/MM/DD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)
	ATO-S Safety Risk Management Office (AJS-2)

6. APPLICATION/INTERRELATIONSHIP
6.1 This Data Item Description (DID) contains the format and content preparation instructions for the O&SHA.

7. PREPARATION INSTRUCTIONS

7.1 Reference documents. The applicable issue of the documents cited herein, including their approval dates and dates of any applicable amendments, notices, and revisions shall be as specified in the contract and in accordance with the SRMGSA in the AMS FAST Toolset.

7.2 Format. The O&SHA format shall be "contractor selected" from either the narrative or tabular styles, as defined in the SRMGSA, Appendix E. Unless the effective presentation would be degraded, the initially selected format must be used for all subsequent submissions.

7.3 Content. The O&SHA is performed by the Contractor primarily to identify and evaluate hazards associated with the interactions between humans and equipment/systems. These interactions include all operations conducted throughout the lifecycle of the system. 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 ensure that operation and maintenance manuals properly address safety and health requirements. The O&SHA is used to both identify new requirements and to support the validation and verification of existing requirements.

The O&SHA shall contain the items shown in the block 7.3.1 through 7.3.11 and be in accordance with the SRMGSA. In addition, each hazard identified shall be listed in either narrative or tabular worksheets (see SRMGSA, Appendix E) that contain, at a minimum, the information described in 7.3.1 through 7.3.11, which shall be included for each identified hazard:

7.3.1 Hazard Number: The hazard identifying numbers will be used to track hazards through validation and verification process to closure. Unique identifying numbers shall be created and marked for individual hazards, or number sequences created for clustered or hazard subsets, and be in accordance with the SRMGSA, Appendix E.

7.3.2 Hazard Description: A complete statement describing the hazard. The Safety Management System Manual, defines a hazard as "… any real or potential condition that can cause injury, illness, or death to people; damage to, or loss of, a system (hardware or software), equipment, or property; and/or damage to the environment." A hazard is a condition that is a prerequisite to an accident or incident.

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

7.3.4 <u>System State</u>: An expression of the various conditions, characterized by quantities or qualities, in which a system can exist. System state is described for each individual hazard associated with the system (e.g., adverse weather and lighting conditions, such as day, dusk, and night). The system state will also include the activity under which the harm may occur (e.g., storage, shipping, installation, testing, maintenance, replacement, decommissioning, or phase of flight, such as en route or taxiing). At a minimum, each hazard must be evaluated for risk in the worst credible system state. Other less critical system states may be evaluated if time permits, but the worst credible system state shall be considered for all hazards at a minimum. A "worst credible" system state assumes the most dangerous (supported by the facts) conditions under which the hazard is postulated to occur. System state shall be in accordance with the SRMGSA, Section 4.0.

7.3.5 <u>Possible Effect</u>: The effect is a description of the potential outcome or harm of the hazard if it occurs in the defined system state.

7.3.6 <u>Severity / Rationale</u>: Severity is determined by the worst credible potential outcome. Less severe effects may be considered analytically in addition to this, but at a minimum, the most severe effects are considered. Do not consider likelihood when determining severity. Determination of severity is independent of likelihood. In additional, to identifying the severity classifications from Table 4.1 Of the SMS Manual, <u>Severity Definitions</u>, and the Rationale for arriving at a specific severity definition must also be included. Refer to the SRMGSA, Section 4.0, for additional information on how to determine risk.

7.3.7 <u>Existing Safety Requirements</u>: The existing safeguards, safety features, protective devices, warnings, training, and procedures that control or eliminate risk. An existing safety requirement is a requirement that exist currently in the FAA (e.g., controls that were previously defined in prior analyses).

7.3.8 <u>Likelihood / Rationale</u>: Likelihood is an expression of how often an event is expected to occur. Severity must be considered in the determination of likelihood. Likelihood is determined by how often the resulting harm can be expected to occur at the worst credible severity. When determining likelihood, the worst credible system states will usually determine the worst credible severity. In additional, to identifying the likelihood classifications from Table 4.3 Of the SMS Manual, <u>Likelihood Definitions</u>, and the Rationale for arriving at a specific likelihood definition must also be included. Refer to the SRMGSA, Section 4.0, for additional information on how to determine risk.

7.3.9 <u>Current Risk / Initial Risk:</u>

Initial. The composite of the severity and likelihood of a hazard considering only verified controls and documented assumptions for a given system state. It describes the risk at the preliminary or beginning stage of a proposed change, program or assessment. Initial risk is determined by factoring both verified controls and assumptions into the system state. When assumptions are made, they must be documented as recommended controls. Once the initial risk is established, it is not changed.

Current. Current risk is the predicted severity and likelihood of a hazard at the current time. When determining current risk, both validated controls and verified controls are factored into the risk assessment. Current risk may change based on the actions taken by the decision-maker that relate to the validation and/or verification of the controls associated with a hazard.

7.3.10 <u>Recommended Safety Requirements:</u> The suggested mitigations or controls that have the potential to mitigate a hazard or risk but have not yet been validated or verified as part of the system or its requirements.

7.3.11 <u>Predicted Residual Risk:</u> Predicted residual risk is the term used until the safety analysis is complete and all safety requirements have been verified. Predicted residual risk is based on the assumption that all safety requirements will be validated and verified.

7.3.12 <u>Safety Risk Management Document</u>: The results of the analysis must be prepared into an SRMD, in accordance with the latest version of the FAA's Safety Management System Manual.

DATA ITEM DESCRIPTION	
1. TITLE **System Safety Assessment Report**	2. IDENTIFICATION NUMBER FAA-DI-SAFT-107

3. DESCRIPTION/PURPOSE

3.1 THE SYSTEM SAFETY ASSESSMENT REPORT (SSAR) is a report to provide management an overall assessment of the risk associated with the system prior to fielding, but also must be employed, prior to operation of the system. This is accomplished by providing summaries of the analyses and testing results. The report contains an overall assessment of the program from the analyses performed and a status of all the existing and recommended safety requirements. The SSAR identifies all safety features of the system, design and procedural hazards that may be present in the system being acquired, and specific procedural controls and precautions that should be followed.

4. APPROVAL DATE (YYYY/MM/DD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) ATO-S Safety Risk Management Office (AJS-2)

6. APPLICATION/INTERRELATIONSHIP
6.1 This Data Item Description (DID) contains the format and content preparation instructions for the System Safety Assessment Report.

7. PREPARATION INSTRUCTIONS

7.1 Reference documents. The applicable issue of the documents cited herein, including their approval dates and dates of any applicable amendments, notices, and revisions shall be as specified in the contract. At a minimum, the SRMGSA shall be used.

7.2 Format. The SSAR format shall be in accordance with the SRMGSA.

7.3 Content. The SSAR includes a summary of the analyses performed and their results, the tests conducted and their results, and the compliance assessment.

5.2.3.6.1.1.1.1 SSAR Format

The SSAR shall contain the following sections:

Signature Page: Include the appropriate signature blocks for Risk Acceptance and SRMD Approval. This must be in accordance with the latest SMS Manual.

1.0 Executive Summary: A brief description of the scope of the assessment. A summary of the assessment findings, including the total number of significant hazards (i.e., high and medium risk hazards), controls, and other significant issues. The total number of safety requirements (both existing and recommended) with requirements listed and discussed.

2.0 Safety criteria and methodology: Provide a narrative summary of the total number of program hazards identified as well as a breakdown of the High Risk, Medium Risk, and Low Risk hazards.

2.1 Risk Assessment Ratings: Results of the analyses are plotted on the Risk Matrix. This is a graphical representation of the hazard breakdown plotted on the Risk Assessment Matrix table.

3.0 Results of analyses and test performed (and other verification activities): Include a summary of the analyzes performed and their results, the tests conducted and their results, and the compliance assessment.

4.0 Hazards Identification:

   4.1 List of all hazards along with specific recommended safety requirements ensuring the safety of the public, FAA personnel, and property. The list of hazards will be categorized as to whether or not they may be expected under normal or abnormal operating conditions.

4.1.1 A statement signed by the contractor system safety manager and the Service Team stating that all identified hazards have been eliminated or controlled and that the system is ready to test, operate, or proceed to the next acquisition phase. In addition, include recommendations applicable to the safe interface of this system with the other system(s).

4.2 Ensure system operations were performed by documenting:

4.2.1 A description or reference of the procedures for operating, testing and maintaining the system. Discuss the safety design features and controls incorporated into the system as they relate to the operating procedures.
4.2.2 A description of any special safety procedures needed to assure safe operations, test and maintenance, including emergency procedures.
4.2.3 A description of anticipated operating environments, and any specific skills required for safe operation, test, maintenance, transportation or disposal.
4.2.4 A description of any special facility requirements or personal equipment to support the system.

Block 7, PREPARATION INSTRUCTIONS (Continued)

4.3 Ensure systems safety engineering was performed by documenting:

4.3.1 A description of or reference to the analyses and tests performed to identify hazardous conditions inherent in the system.
4.3.2 A discussion of or reference to the results of tests conducted to validate safety criteria requirements and analyses.

5.0 List of hazards (with risk) identified to date: A list of all hazards by subsystem or major component level that have been identified and considered from the inception of the program in an appendix to this SSAR:

5.0.1 A discussion of the hazards and the actions that have been taken to eliminate or control these items.
5.0.2 A discussion of the effects of these safety requirements on the probability of occurrence and severity level of the individual hazards.
5.03 A discussion of the residual risks that remain after the recommended safety requirements are applied or for which recommendations could not be applied.

6.0 SRVT: Provide an updated list of safety requirements that have been verified and a status of the requirements that need to be verified and when they will be verified.

MM/DD/YYYY	Previous editions are obsolete	Page 3 of 3

K.1 Operational Safety Assessment

The OSA is a systems engineering practice of developing coordinated, systematic safety objectives and requirements for the overall system (including procedural considerations) early in the development phase. It is a development tool based on the assessment of hazard severity.   The OSA also establishes how safety requirements are to be allocated between air and ground components and how performance and interoperability requirements might be influenced.

- The OSA is completed during the Mission Analysis Phase and the results are incorporated into the Enterprise Architecture, the preliminary Program Requirements, and Investment Analysis Plan (IAP).

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

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

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

- The ASOR analysis is a process of using hazard severity to determine the safety objectives and requirements of the system. Its purpose is to establish requirements that ensure the probability of a hazard leading to an accident has an inverse relationship to the accident's severity or consequence.

- A report summarizing the analysis and resulting requirements should be included up front in the OSA. See Appendix B for an example of an OSA outline. See Appendix C for an example of an OSA worksheet.

- The OSA is conducted by service team personnel, reviewed in accordance with the Service unit process, and forwarded to the ATO SSWG for review and concurrence. The OSA analysis is documented in an SRMD.

- The OSA analysis must include all the information depicted in the format in Appendix C. The results of the OSA will be briefed to the JRC upon request by the EC or JRC.

K.2 Comparative Safety Assessment (CSA)

The CSA is a safety analysis that provides 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 is used by the BCAT and Business Case Evaluation Team (BCET) to rank the options for decision-making by the program. The CSA is reviewed by the ATO SSWG, and then forwarded for final review and approval in accordance with the SMS Manual, latest revision. See Appendix H for the CSA template.

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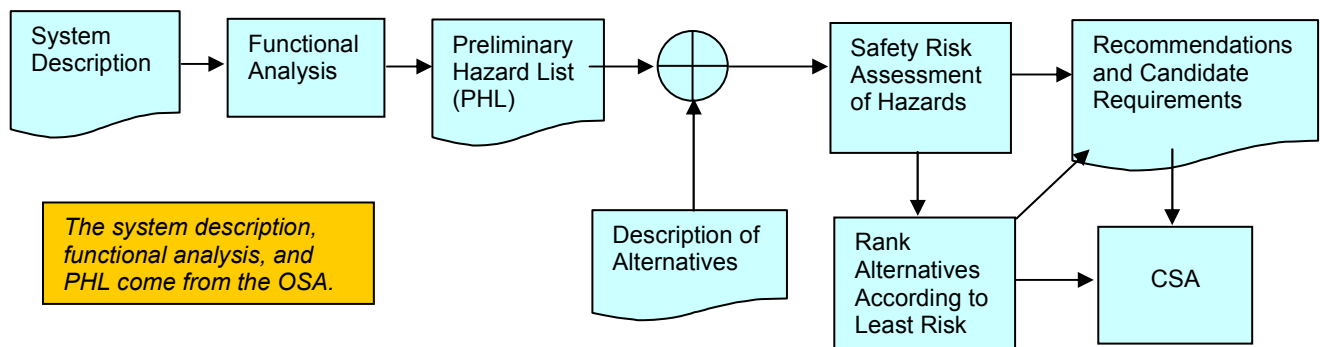

Figure K-1 CSA Process Flow

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

Service Team personnel conduct the CSA with the guidance of the ATO SSWG Chair. The CSA is reviewed in accordance with the Service unit process, and submitted to the ATO SSWG as a subset of the SRMD. The results of the CSA will be briefed at the JRC if it was a factor in selecting the chosen option.

K.3 Preliminary Hazard Analysis (PHA)

The PHA is the initial effort in risk assessment of the selected system. The purpose of the PHA is not to affect control of all hazards because sufficient information may not be available. Its purpose is to make an early identification of the hazards, hazardous system states (with all of the accompanying system implications), and safety requirements. The output of the PHA is used in: (1) further developing system safety requirements to be added to the System Safety Requirements List, (2) preparing performance/design specifications, and (3) initiating the hazard tracking and risk resolution process.

When required by the PSP, the PHA shall be conducted after the alternatives are evaluated and a single alternative is selected as the best option. For the AMS this means it will be done after the CSA and before the FID. The PHA subset of the SRMD shall be completed and approved prior to the JRC Secretariat's cut-off date for the decision. Appendix E contains the format for documenting the PHA.

A PHA must include, but not be limited to, the following information:

- As complete a description as possible, from the program, of the system or systems being analyzed, how it will be used, and interfaces with existing and developing systems

- The OSED established during pre-development (This forms the basis for a system description but should be updated to include additional details as they become available.)

A review of historical safety experience (lessons learned on similar systems)Identification of the safety requirements and other regulations pertaining to personnel safety, environmental hazards, and toxic substances with which the system must comply (Note: the purpose of considering these hazards is to identify any hazard that may impact NAS safety.)

- A Preliminary Hazard List

- A list of causes for each hazard

- For each hazard, an evaluation of the worst credible outcome under various system states

- For each hazard, an assessment of the potential effects of the hazard in the system state

- For each hazard, a list of existing requirements

- An updated SRVT (Section 5.2.12, Appendix G)

- Recommendation(s) for additional safety requirements or other corrective actions

The BCAT or BCET will brief the results of the PHA to the JRC in order to proceed with an Investment Decision. This briefing will be coordinated with the Service Team.

K.4 Program Safety Plan (PSP)

A PSP is developed and tailored specifically for each program using this SRMGSA and is available on the ATO SSWG KSN website. Contact ATO Office of Safety to

gain access. The PSP is the government's plan for program safety and will be used to ensure compliance with provisions of the SRMGSA. It forms the basis for the contractor's corresponding System Safety Program Plan (SSPP), which typically is contractually required per the DID FAA-DI-SAFT-102, shown in Appendix J of this SRMGSA. A definition of planned safety work to be completed during CRD is to be included in the CRD Plan. This part of the CRD documents the agreement reached in the Safety Strategy meeting with the ATO SSWG Chair.   At the completion of the CRD phase, the IAP and pPR will define the safety work to be performed during IA to support the IID and FID. These documents need to be completed and approved prior to the JRC Secretariat's cut-off date for that decision.

The Contractor's SSPP, when reviewed and approved, by the ATO SSWG Chair, is a contractually binding agreement between the FAA and a contractor on how and when the contractor intends to meet the specified PSP requirements. (SRM approval of the SSPP does not constitute acceptance on behalf of the FAA program office.   That is the responsibility of the Service Team.)   The plan details the contractor's program scope, safety organization, program milestones, requirements and criteria, hazard analyses, safety data, safety verification, audit program, training, accident/incident reporting, and interfaces.

The PSP is an input to and an integral part of the Service Team's Implementation Strategy and Planning document, Section 5.5. Each tailored PSP should use the outline shown in the PSP template.

The PSP is developed during IA by the Service Team , or other entity as recommended by the SRM representative on the IAT (with team lead's concurrence) , reviewed in accordance with the Service Unit process, and is submitted to the ATO SSWG for approval and then to the Director of SMS for concurrence.

The BCAT or BCET will brief the JRC regarding the contents and tailoring of the PSP and include an assessment of the PSP's ability to meet the requirements of FAA Order 8040.4, AMS 4.12, and the guidance of the SRMGSA.

At a minimum the PSP covers:

- Program scope and objectives

- Roles and Responsibilities

- System safety organization

- System safety program milestones

- General system safety requirements and criteria

- Hazard analyses to be performed

- Hazard tracking system processes to be used

- System safety data to be collected

- Safety requirements management (including how to manage the SRVT)

- Safety assessments and reports for changes to program, design, and engineering

- System safety training required

- System safety interfaces with design engineering, contractors, management, and other specialty engineering groups

- PSP management of cost and schedules

- PSP interfaces with other program plans

K.5 Sub-System Hazard Analysis (SSHA)

The general purpose of the Sub-System Hazard Analysis (SSHA) is to perform a safety risk assessment of a system's sub-systems/components at a more detailed level than that provided in a PHA. The specific purposes of the SSHA are:

- Verify sub-system compliance with system/safety requirements

- Identify previously unidentified hazards associated with the sub-system

- Assess the risk of the sub-system design

- Consider human factors, functional and component failures, and functional relationships between components comprising the sub-system, including software

- Recommend actions to control the hazards

- Update the SRVT

The hazards identified by an SSHA can be documented in either a narrative or tabular format. Examples of the tabular format are provided in Appendix E.

K.6 System Hazard Analysis (SHA)

The general purpose of the SHA is to perform a detailed safety risk assessment of a system; in particular, (1) the interfaces of that system with other systems, and (2) the interfaces between the sub-systems that compose the system under study.

The specific purposes of the SHA are:

- Verify system compliance with safety requirements in the system specification

- Identify previously unidentified hazards associated with the system interfaces, and system functional faults, and system operation in the specified environment

- Assess the risk of the total system design

- Consider human factors, system/functional failures, and functional relationships among sub-systems comprising the system, including software

- Identify existing requirements

- Update the SRVT

- Recommend additional requirements.

The hazards identified by an SHA can be documented in either a narrative or tabular format. An example of the tabular format is provided in Appendix E.

K.7 Operating & Support Hazard Analysis (O&SHA)

The general purpose of the Operating & Support Hazard Analysis (O&SHA) is to perform a detailed safety risk assessment of a system's operational and support procedures.

The specific purposes of the O&SHA are:

- Evaluate operating and support procedures for a given system

- Identify hazards associated with those procedures

- Consider human factors and critical human errors, normal and emergency operations, and support tasks that may adversely affect NAS safety.

- Assess the risk associated with those hazards

- Identify safety requirements in existing FAA documents (e.g., Orders, FARs)

- Update the SRVT

- Develop alternative controls and/or procedures to eliminate or control the hazards

The O&SHA is performed to identify and evaluate the hazards associated with the environment and personnel throughout the lifecycle of a system/element. The O&SHA identifies and evaluates hazards resulting from the implementation of

operations or tasks performed by persons considering biotechnological factors, regulatory or contractually specified personnel safety and health requirements.

The hazards identified by an O&SHA are documented in either a narrative or tabular format. An example of the tabular format is provided in Appendix E.

K.8 Test Safety Analysis (TSA)

AMS no longer allows programs to become operational without going through the JRC process, which includes developing the Exhibit 300 program Baseline and completing the JRC Readiness Review Checklist for the decision being sought. Research and development (R&D) and spiral development programs will meet with the JRC Secretariat's office and stakeholders (including SMS and system safety representatives) to develop a strategy to transition the R&D or spiral program to one that complies with the AMS and SMS.

While programs are in the R&D phase, the best approach to system safety assessments as specified by the SMS is to develop an PSP and conduct an OSA during the early phases of the program. This lays the foundation for future system safety work by the completion of a safety plan, functional analysis, the target level of safety (TLS), and preliminary hazard list (PHL). This assessment and other safety work considered or done, shall be accomplished under the principles of this SRMGSA and will include reviews by the ATO SSWG and concurrence by its Chair.

Test Safety Assessment –
For a site-specific application such as an OPEVAL or Demonstration project, a Test Safety Assessment is required. Such testing requires the development and use of a Test Safety Analysis (TSA) to consider the safety of the test itself. Safety engineers need to work closely with test planners to ensure that proper precautions are observed during the testing to prevent personnel injury or equipment damage. Each proposed test needs to be analyzed by safety personnel to identify hazards inherent in the test and to ensure that hazard control measures are incorporated into test procedures.

It is during the process of test safety analysis that safety personnel have an opportunity to identify other data that may be useful to safety and can be produced by the test with little or no additional cost or schedule impact.

When an R&D or spiral development project is targeted for wide application within the NAS, either through the mandated acquisition process or NAS Change Control Board (NAS CCB), a PHA is typically required. Regardless of the JRC or EC decision being sought, the process identified in this SRMGSA must be followed.

It is the responsibility of the Service Team, or R&D development team to conduct the PSP, OSA, TSA, or PHA as appropriate. Again, these safety analyses/assessments must be submitted to the ATO SSWG for concurrence. Table M-1 describes the process for R&D and spiral development programs. The indicated steps should be accomplished before the program enters the formal AMS and JRC process so that when it meets with the JRC Secretariat's office and stakeholders, much of the work required for the JRC or EC decision already will be complete or nearly so.

Table K-1 Safety Assessment Process for R&D and Spiral Development Programs

Program Type and Phase	Safety Assessment	Hazard Tracking and Risk Resolution	Responsibility to Prepare	Approval Needed	Risk Acceptance
Early R&D	Program Safety Plan and Operational Safety Assessment	Put all hazards in HTS and Track to Closure (M&H)	Product, Project or R&D Team	ATO SSWG concurs	Per SMS Manual, Latest Revision
Site Specific Opeval or Demonstration	Test Safety Assessment	Put all hazards in HTS and Track to Closure (M&H)	Product, Project or R&D Team	Chair, ATO SSWG	Per SMS Manual, Latest Revision
Wide Application	PHA	Put all hazards in HTS and Track to Closure (M&H)	Product, Project or R&D Team	ATO SSWG concurs	Per SMS Manual, Latest Revision

K.9 System Safety Assessment Report (SSAR)

The general purpose of the SSAR is to perform and document a comprehensive evaluation of the accident risk being assumed before deployment of a system to the field. This means that the SSAR summarizes all of the safety analyses and assessments conducted on the program up to that point. The SSAR will address the completion of the verification process. It contains the Safety Action Records updated to show the validation and verification status of all safety requirements, mitigations and/or controls for each of the hazards. It also contains the SRVT. The SRVT contains all of the safety requirements identified in prior safety analyses and assessments with the origin of the requirement (e.g.,, OSA, CSA, PHA, SHA). At the ISD, all safety requirements must be validated and verified by the Service Team. Objective evidence of V&V closed status may be reviewed by the ATO SSWG upon request.

The specific purposes of the SSAR are to:

- Summarize the results of SRM on the program

- Identify all safety features of the hardware, software, and system design

- Identify procedural, human factors, hardware, and software related hazards that have been identified in the program to date

- Contain all SARs with the associated safety requirements, controls and mitigations

- Update the SRVT to show the validation and verification status of each safety requirement

- Assess system readiness, based on cumulative safety risk, to proceed on with deployment of the system

The V&V status of requirements summarized in the SSAR is accomplished through one or more safety reviews. The types of safety reviews are as discussed below:

K.9.1 Periodic Review

These are safety reviews conducted throughout the life of a program. They evaluate the status of hazards based on the verification of mitigating requirements. Because they are based on the verified requirements, hazards closed during the review are completed and do not need to be revisited. Frequency of periodic reviews must be specifically defined.

K.9.2 Phased Review

These are reviews held for defined portions of systems undergoing implementation into the NAS. Phased Reviews apply to a single JRC decision, in that a single JRC decision encompasses implementing a system in steps, or phases. The program itself does not need to use the term "phased" in its title. As long as the implementation is incremental or in steps, each increment or step (hereinafter called phase) will have safety reviews. The reviews evaluate the status of hazards based on the verification of mitigating requirements for that particular phase. Because reviews are based on the phases, hazards closed during the review may only be closed for that phase and may be subsequently reviewed during succeeding phases or in the Final Implementation Review (FIR).

K.9.3 Final Implementation Review

These are reviews conducted for a program's ISD. The reviews evaluate the status of hazards based on the verification of mitigating requirements of the program for that JRC decision.   Because hazards are based on the state of the implementation of requirements prior to the ISD, and because the final JRC decision is being made, hazards closed during this FIR are completed. This FIR may review hazards, previously closed or not, from a Phased Review, because those reviews were not necessarily based on the program's final state.

Hazards with mitigating requirements not verified at ISD must be updated as "Monitor" (see Table 5.2-2). The mitigation and verification plan for those hazards must be approved by the ATO SSWG as part of the I SSAR and must be included in the briefing to the ISD decision maker. An outline of an SSAR is contained in Appendix F.

The results of the SSAR will be briefed by the Service Team to the JRC as a part of the ISD.

The status of each SAR is defined by the guidelines in Table K-2.

Table K-2 SAR Status Definitions

Status	Definition
Proposed	Hazard identified and SAR written. SAR has not been reviewed and approved by the ATO SSWG.
Open	SAR approved by the ATO SSWG. Mitigation and verification plan not developed.
Monitor	SAR approved by the ATO SSWG. Mitigation and verification plan for the SAR exists and is approved by program management. Awaiting results of the Mitigation and verification plan.
Recommend Closure	All mitigation and verification actions are complete. SAR is awaiting review by the ATO SSWG, where status and residual risk determination is made.
Closed	No further action to be taken. SAR is closed by the ATO SSWG. SAR forwarded to Director of SRM for review and coordination of risk acceptance by the appropriate management activity.

K.10 Safety Requirements Verification Table (SRVT)

The SRVT is an evolving list of safety requirements that is started with the first safety assessment (usually the OSA or PHA) and ends with the SSAR that contains all safety requirements identified prior to ISD. Safety Requirements are controls written in requirements language[7]. Safety requirements are used to control hazards and all requirements must be identified as such in the program's requirements documents. Changes to safety requirements must be reported to the program's SRMP and, if necessary, to the ATO SSWG. The SRVT contains a list of requirements and objectives (i.e., controls that do not meet the criteria for a requirement, design constraints, and statements of work) that are identified in the safety assessments performed on a program. The SRVT contains the following information:

- List of requirements and objectives identified in any safety assessment for a given program

- The source of the requirement (e.g.,, OSA, PHA, CSA)

- Validation and verification information

- The level of risk controlled by the requirement

The SRVT will be used to accomplish the Validation and Verification process for the safety requirements. For more information on conducting Validation and Verification, see the FAA System Engineering Manual (SEM). Per the SMS Manual and the SEM, validation is the

---

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

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

The format to be used for the SRVT is shown in Appendix G. The operational organization (i.e., Service Team) must assure that all requirements are captured within the Verification Requirements Test Matrix (VRTM).

The SRVT is intended to provide a continuing list and status of requirements and objectives that result from the SRM process. The requirements that are contained in this list must meet the standards detailed in the FAA SEM chapter on "Requirements Management."

K.11 System Safety Program Recommendations (SSPR)

The SSPR is a summary document that the ATO SSWG Secretariat prepares for the program. It is separate from the SRMD or SRMDM. This document summarizes the ATO SSWG conclusions related to each safety analysis, assessment, report, or program plan that it reviews. This document transmits the ATO SSWG findings and conclusions to the Director of SRM for transmittal to the Service Team. The SSPR can be an official letter or report. The SSPR should be as short as possible, but must contain the following information:

- Name of the program, Service Teams name and office, and the type of analysis, assessment, report, or plan that the ATO SSWG reviewed

- Summary indication of concurrence/non-concurrence with the document

- Summary of findings and conclusions of the ATO SSWG

- Recommendations of the ATO SSWG

L.1 Software Safety Analyses (SwSA)

The purposes of the SwSA are to:

- Identify, generate, verify, and validate software safety requirements.
- Identify and banner all safety-critical Computer Software Configuration Items (CSCIs) that control or influence safety-critical hardware/system functions.
- Analyze safety-critical CSCIs and their system interfaces as designed and implemented for events, faults, and environments that could cause or contribute to undesired events affecting safety both within the system under analysis and all interfacing systems.
- Analyze the implementation of software safety design requirements to ensure that it accomplishes the intent of the requirement and achieves the targeted residual risk level. The analysis will verify that there is no single point or likely multiple failures that could compromise the safety feature.
- Ensure the implementation of software safety requirements will not introduce new hazards or adversely affect other safety requirements.
- Ensure that the actual coded software does not cause identified or unidentified hazards to occur or inhibit desired functions, thus creating hazardous conditions.
- Perform code analysis and code reviews of all safety-critical software components.
- Ensure that software effectively mitigates end-item, hardware/system-hazardous anomalies where possible.
- Ensure that software safety design requirements are thoroughly tested, including fault injection testing, stress testing, duration testing, out-of-bounds testing and data limit testing.
- Ensure all software Safety-Critical Requirements are traceable from the specifications, through design, and test.
- Ensure all software safety-critical trouble reports are identified as such and are subjected to the SwSA.

L.2 Severity versus Risk Based Software Safety Assurance Levels

There are numerous CNS/ATM hazards, which do not directly influence or contribute to hazards within or to an aircraft that must be mitigated. RTCA/DO-278 is concerned with all software-controlled systems within the NAS (e.g., surveillance radars, weather radars, navigation systems, surface management systems, air traffic management systems). The assignment of assurance levels for software is based on the severity and likelihood of system hazards. Design mitigation allows for flexibility in managing system risk that may be influenced by software. Therefore, by translating a specified assurance level from the initial System Risk via the SwAL assignment matrix, an acceptable level of assurance can be specified for the system's software. An example is the anomalous behavior of the software controlling radiation cut-outs of a ground radar system, which could result in

inadvertent radiation to ground/maintenance personnel. For these, non-aircraft specific hazards, all columns and rows contained within Figure 4.2-3 in Section 4.2.14 must be used.

The SwAL assignment is a safety-critical management decision. Failure to assign a high enough level initially could force the development community to build the artifacts required by the RTCA/DO-178B and DO-278 objectives after the fact. Retroactive generation of artifacts from the development process is never cost, schedule, engineering, or safety effective. Additionally, the FAA and contractor management personnel may decide that the development of an "AL2" program, for example, would be cost and schedule prohibitive, thus necessitating design and architectural mitigation techniques as previously stated in Section 4.3's discussion on using the Safety Order of Precedence. For an example of selecting different assurance levels for airborne and ground portions of the same systems, the Figure below illustrates an extremely simplistic architectural mitigation example of two possible solutions.
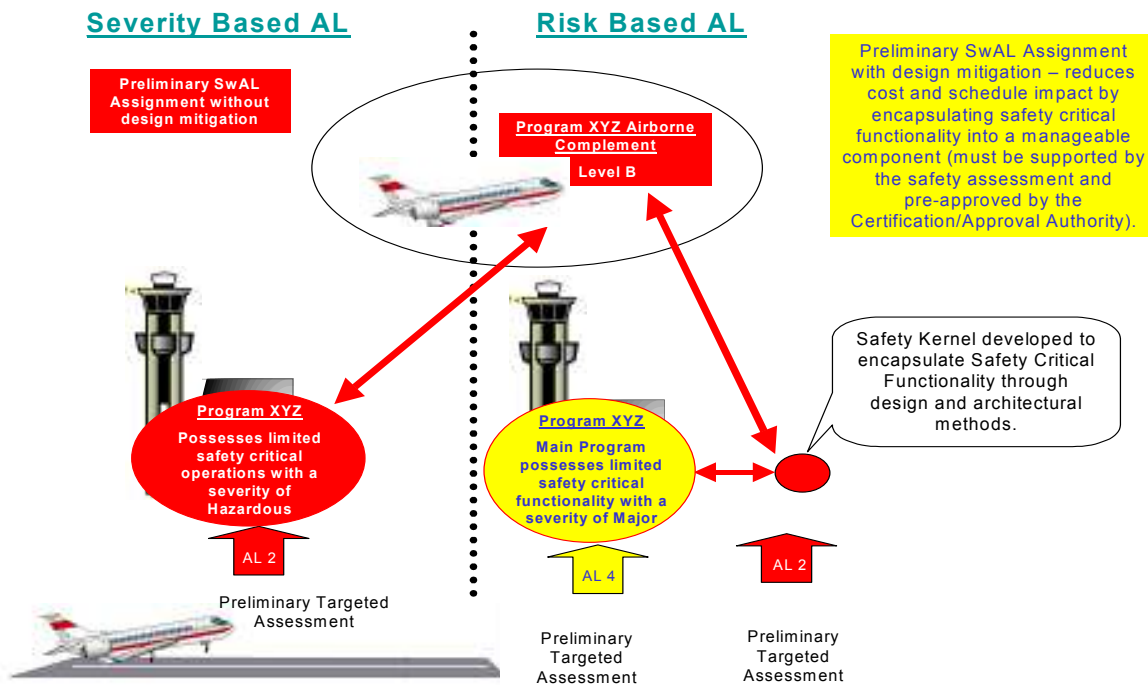

Figure L-1 SwAL Assignment/Architectural Decisions

In this example, the FAA and contractor management personnel may decide that the development of an "AL2" program for the airborne component would be cost and schedule appropriate, while the development of an "AL4" program would be appropriate for the ground component, thus necessitating design and architectural mitigation techniques as previously stated in Section 4.3's discussion on using the Safety Order of Precedence. This decision reduces the cost and schedule impact by encapsulating safety critical functionality into a manageable component.

L.3 Air Traffic (ATO) versus Certification (AVS) SRM Equivalent Processes

Many systems under development blur the lines between aircraft and ground systems. These highly integrated systems require a conjunction between the system development role of the ATO and the aircraft/operation certification role of AVS. The ATO operates a two-party safety system. AVS operates in a three party safety system (see figures below). In the AVS system, there are three parties to the certification of an aircraft or operation: (1) the applicant seeking certification, (2) the public who will use the certified service, and (3) the FAA as the certification authority. In the ATO system, there are two parties: (1) the FAA as the acquisition and using authority, and (2) the contractors and suppliers of the equipment and procedures. The AVS process is governed by public law documented in the Federal Aviation Regulations (FAR), Advisory Circulars, AMS and SMS. The ATO process is guided by the AMS, FAA Orders, the SMS Manual, and this SRMGSA. While the two systems differ in terminology and process, there are many similarities: (1) the identification of hazards/failure conditions, causes, and effects, (2) assessment of risk, and (3) validation and verification of safety requirements.
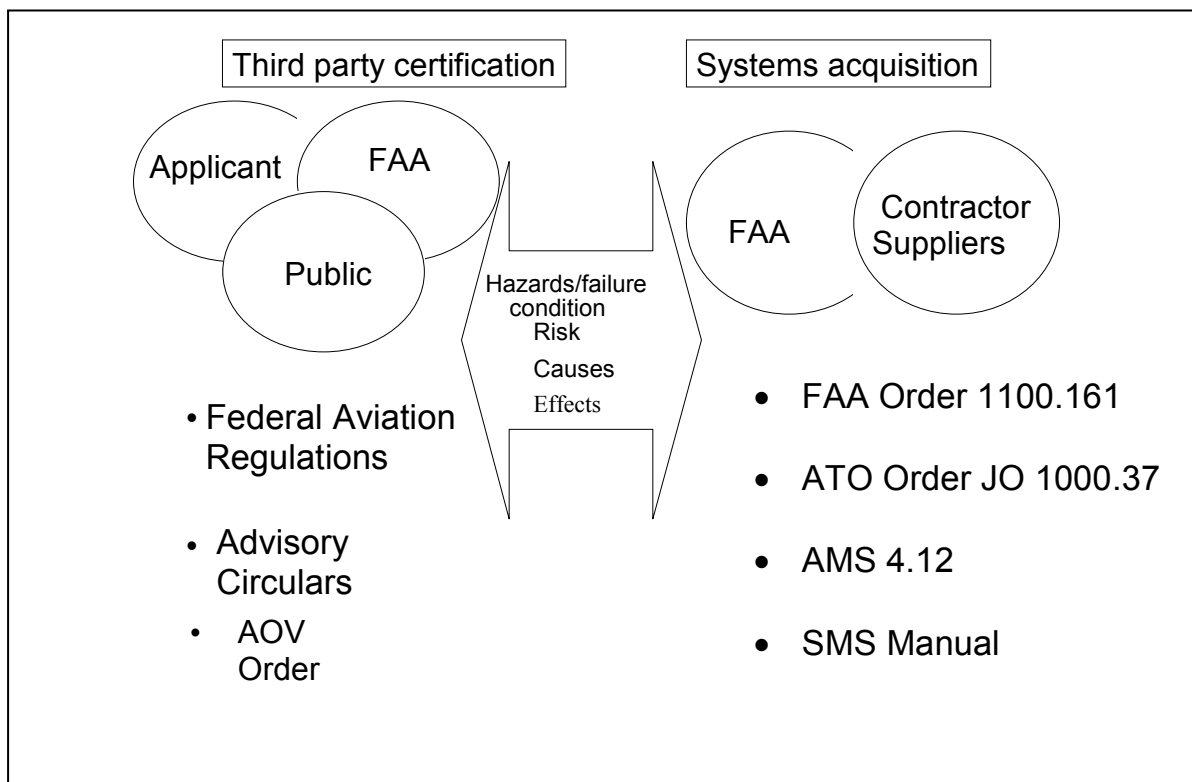
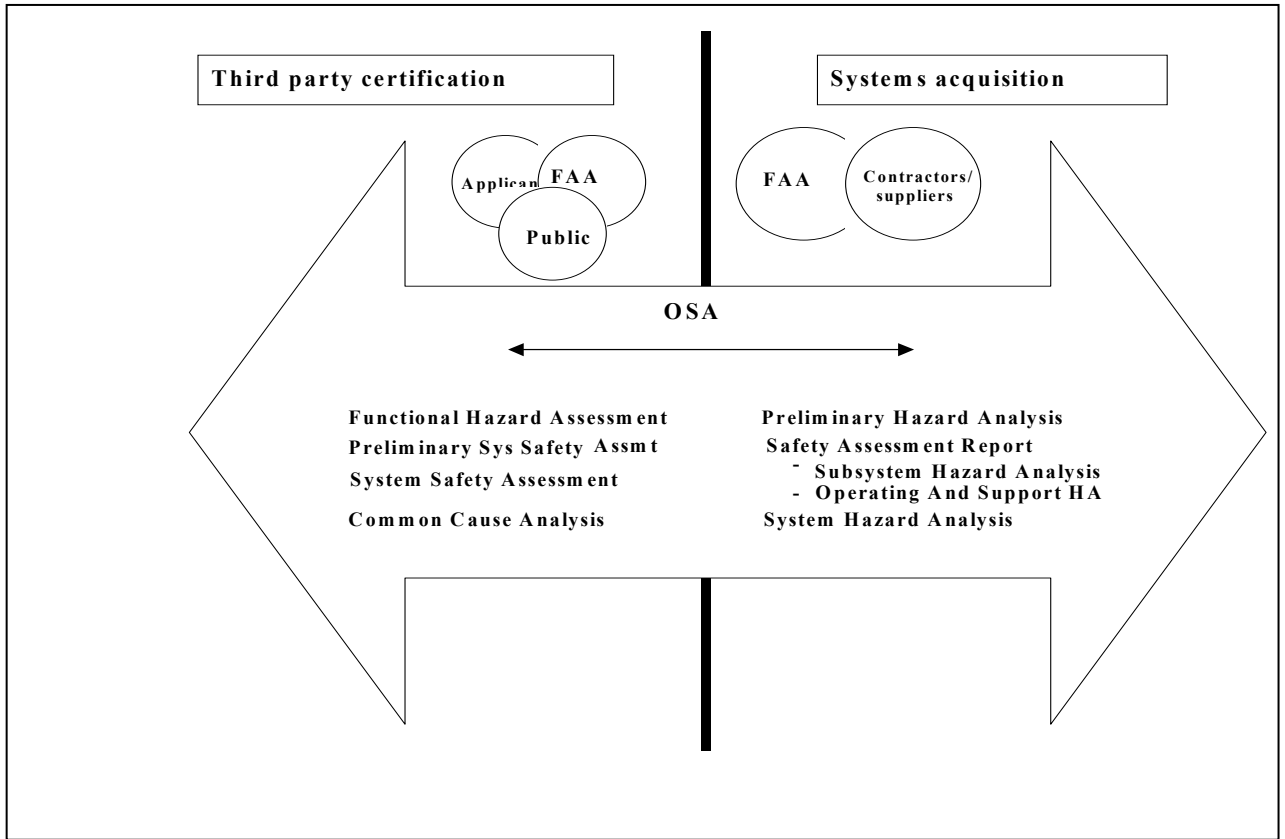

Figure N-2 Equivalent Processes

Figure L-3 Equivalent Analysis

The ATO and AVS processes, if conducted properly, can improve cross-functional communication within the FAA, resulting in both AVS and the ATO benefiting from each other's work. The ATO has adopted AVS definitions of severity and likelihood. Therefore, when hazards are identified and risk assessed, the risk classification means the same thing to both the ATO and AVS. The processes that each uses are very similar and can support the roles of both the ATO and AVS in the development of highly integrated air and ground systems. The equivalency and integration of the ATO and AVS safety analyses are depicted in the figure above. It should be noted that in the three-party AVS system the applicant performs the analyses, while in the two-party ATO system it is often the FAA or its contractors that perform the safety analyses.

Appendix M: Acronyms

Acronym	Abbreviated term
AC	Advisory Circular
AMS	Acquisition Management System
AOV	Air Traffic Safety Oversight
ASAG	Acquisition System Advisory Group
ASOR	Allocation of Safety Objectives and Requirements
ATC	Air Traffic Control
ATM	Air Traffic Management
ATO	Air Traffic Organization
AVS	Office of Aviation Safety
BCAR	Business Case Analysis Report
CNS	Communication, Navigation, Surveillance
CRD	Concept and Requirements Definition
CSA	Comparative Safety Assessment
EC	Executive Council
FAA	Federal Aviation Administration
FAST	FAA Acquisition System Toolset
FID	Final Investment Decision
HTRR	Hazard Tracking and Risk Resolution
HTS	Hazard Tracking System
IA	Investment Analysis
IAP	Investment Analysis Plan
IAT	Investment Analysis Team
IID	Initial Investment Decision
ISD	In-Service Decision
ISM	In-Service Management
ISP	Implementation Strategy and Planning
JRC	Joint Resources Council
LOB	Line of Business
MA	Mission Analysis

NAS	National Airspace System
O&SHA	Operating and Support Hazard Analysis
OSA	Operational Safety Assessment
OSU	Operational Service Unit
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
pPR	Preliminary Program Requirements
PR	Program Requirements
PSP	Program Safety Plan
RAC	Risk Assessment Code
RCC	Readiness Criteria and Checklist
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automotive Engineers
SAR	Safety Action Record
SHA	System Hazard Analysis
SI	Solution Implementation
SMS	Safety Management System
SRM	Safety Risk Management
SRMD	Safety Risk Management Document
SRMDM	Safety Risk Management Decision Memo
SRMGSA	Safety Risk Management Guidance for System Acquisitions
SRVT	Safety Requirements Verification Table
SSAR	System Safety Assessment Report
SSHA	Sub-System Hazard Analysis
SSMP	System Safety Management Program
SSPP	System Safety Program Plan
SSPR	System Safety Program Recommendations
SSWG	System Safety Working Group
SwAL	Software Assurance Level
SwSA	Software Safety Analysis