Chapter 2: System Safety Policy and Process

2.1 FAA POLICIES 2

2.2 THE FAA SAFETY RISK MANAGEMENT PROCESS 3

2.0 System Safety Policy and Process

This section describes the System Safety policies and processes used within the FAA.

2.1 FAA policies

The primary policy governing safety risk management and system safety is formal in the FAA. Order 8040.4 and the Acquisition Management System (AMS). Note there are many other orders associated with safety. When it is applicable to discuss them, the appropriate reference has been provided in the applicable section.

2.1.1 FAA Order 8040.4

This order sets requirements for the implementation of safety risk management within the FAA and establishes the FAA Safety Risk Management Committee (SRMC).

Safety risk management

The order requires the FAA-wide implementation of safety risk management in a formalized, disciplined, and documented manner for all high-consequence decisions. Each program office and Line of Business (LOB) is required to establish and implement the policy contained within Order 8040.4 consistent with that office's role in the FAA. While the methods and documentation requirements are left to the program office's discretion, each is required to satisfy the following criteria:

Plan: The safety risk management process shall be predetermined, documented in a plan that must include the criteria for acceptable risk.
Hazard identification: The hazard analyses and assessments required in the plan shall identify the safety risks associated with the system or operations under evaluation.
Analysis: The risks shall be characterized in terms of severity of consequence and likelihood of occurrence in accordance with the plan.
Comparative Safety Assessment: The Comparative Safety Assessment of the hazards examined shall 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 shall include the safety Comparative Safety Assessment. Comparative Safety Assessments may be used to compare and contrast options.

The order permits quantitative or qualitative assessments, but states a preference for quantitative. It requires the assessments, to the maximum extent feasible, to be scientifically objective, unbiased, and inclusive of all relevant data. Assumptions shall be avoided when feasible, but when unavoidable they shall be conservative and the basis for the assumption shall be clearly identified. As a decision tool, the Comparative Safety Assessment should be related to current risks and should compare the risks of various alternatives when applicable.

In addition, the order requires each LOB or program office to plan the following for each high-consequence decision:

Perform and provide a Comparative Safety Assessment that compares each alternative considered (including no action or change, or baseline) for the purpose of ranking the alternatives for decision making.
Assess the costs and safety risk reduction or increase (or other benefits) associated with each alternative under final consideration.

Safety Risk Management Committee

The SRMC is established by the Order to provide guidance to the program offices or LOBs, when requested, on planning, organizing, and implementing Order 8040.4. The SRMC consists of technical experts in safety risk management, with representation from each Associate/Assistant Administrator and the Offices of the Chief Counsel, Civil Rights, Government and Industry Affairs, and Public Affairs.

2.1.2 AMS Policies

The AMS policy contains the following paragraphs in 2.9.13:

System Safety Management shall be conducted and documented throughout the acquisition management lifecycle. Critical safety issues identified during mission analysis are recorded in the Mission Need Statement; a system safety assessment of candidate solutions to mission need is reported in the Investment Analysis Report; and Integrated Product Teams provide for program-specific safety risk management planning in the Acquisition Strategy Paper.

Each line of business involved in acquisition management must institute a system safety management process that includes at a minimum: hazard identification, hazard classification (severity of consequences and likelihood of occurrence), measures to mitigate hazards or reduce risk to an acceptable level, verification that mitigation measures are incorporated into product design and implementation, and assessment of residual risk. Status of System Safety shall be presented at all Joint Resources Council (JRC) meetings. Detailed guidelines for system safety management are found in the FAST.

2.2 The FAA Safety Risk Management Process

The FAA Safety Risk Management process is designed to evaluate safety risk throughout the National Airspace System (NAS) life cycle. The primary focus of this process is to identify, evaluate, and control safety risk in the NAS. Each LOB or program office has unique responsibilities in the NAS. As a reflection of these responsibilities, the safety risk management program and the associated assessment tools/techniques used by each office will be different from the other LOBs. The overall approach will remain the same: early identification and control of those hazards that create the greatest risk within the NAS. The following paragraphs summarize each office's approach to system safety risk management.

The safety risk management process operates as an integral part of the AMS under the oversight of the FAA System Engineering Council. Figure 2-1 depicts the AMS Integrated Product Development System (IPDS) process and the supporting system safety activities. The details of "how" to perform each activity shown in this diagram are discussed in later chapters. General guidance for AMS safety activities is contained in the NAS System Safety Management Plan (SSMP).

System Safety Products in the AMS Life Cycle

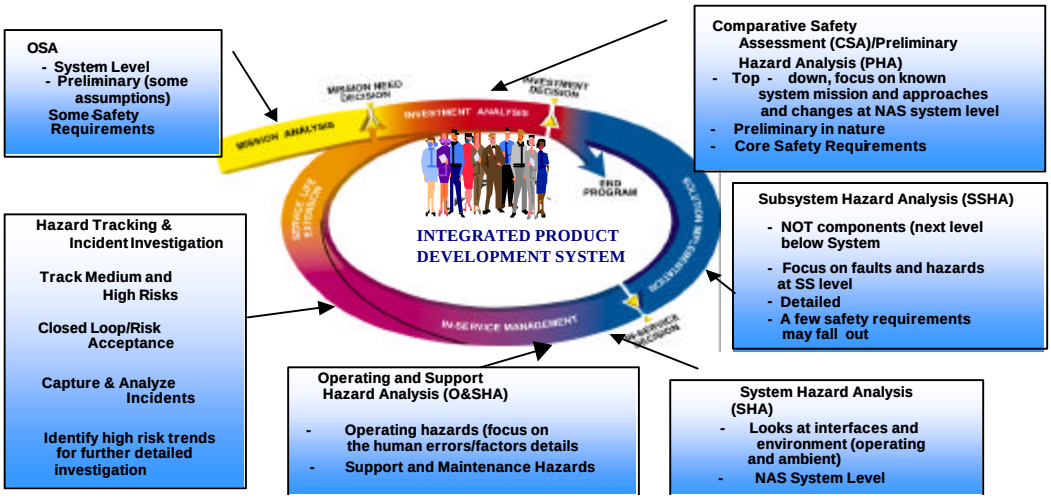

Figure 2-1: Integrated Product Development System

The prime goal of the AMS system safety program is the early identification and continuous control of hazards in the NAS design. The NAS is composed of the elements shown in Figure 2-2.

The outputs of the AMS system safety process are used by FAA management to make decisions based on safety risk. These outputs are:

Operational Safety Assessment (OSA) Operational Safety Requirements (OSR) Comparative Safety Assessments (CSA) Preliminary Hazard Analyses (PHA) Subsystem Hazard Analyses (SSHA) System Hazard Analyses (SHA) Operation and Support Hazard Analyses (O&SHA) Hazard Tracking and Risk Resolution (HTR) Other appropriate hazard analyses. (See Chapters 8 & 9)

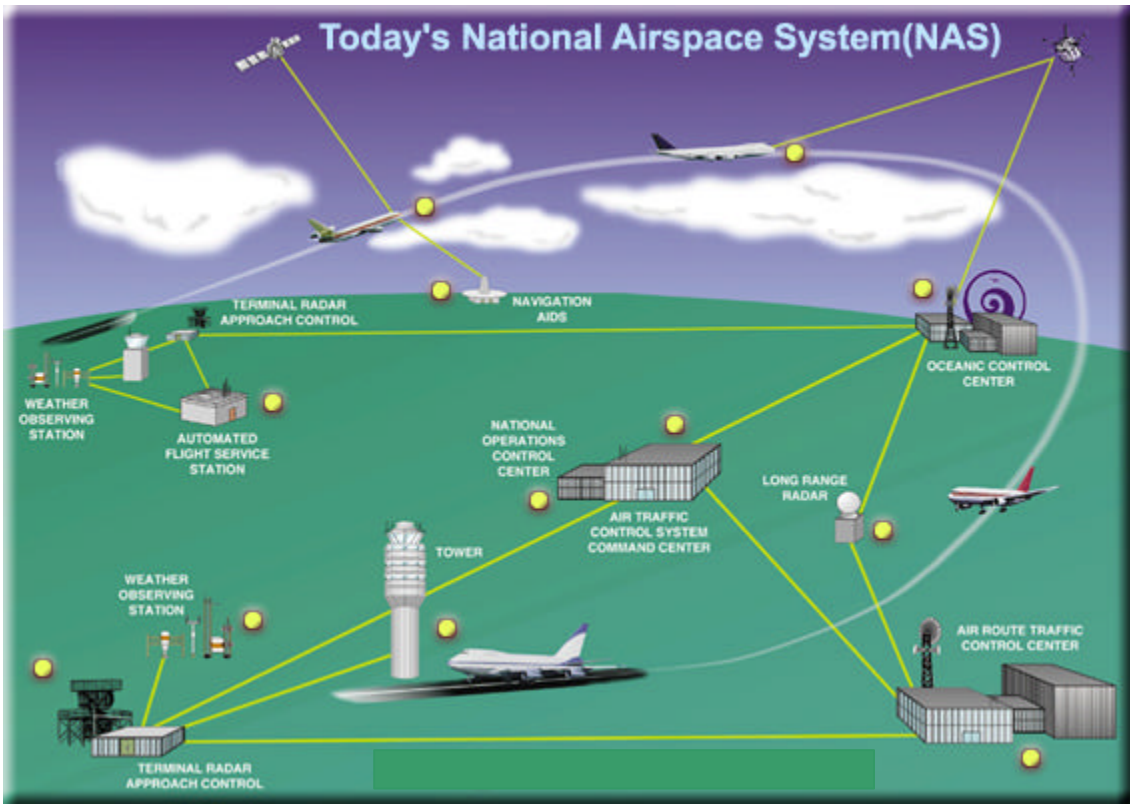

Figure 2-2: Elements of the National Airspace System

2.2.1 Integrated Product Development System and Safety Risk Management Process

Figure 2-1 depicts the integrated product development system process and the supporting system safety activities. The integrated product development system is broken down into a number of life cycle milestones which include: Mission Analysis, Investment Analysis, Solution Implementation, In Service Management, and Service Life Extension. As noted in Figure 2-1, system safety activities will vary depending on the phase of the life cycle. The OSA is to be conducted during mission analysis, prior to the mission need decision at JRC-1. During investment analysis, initial system safety analysis is further refined into Comparative Safety Assessment and a Preliminary Hazard Analysis (as needed). After the investment analysis, more formal system safety activities are initiated by the product teams for that program and in

accordance with the NAS SSMP. During solution implementation, a formal system safety program plan is to be implemented. System safety activities should include system and sub-system hazard analysis. Prior to the in-service decision, operating and support hazard analysis is conducted to evaluate the risks during in-service management, and service life extension.

Operating and Support Hazard analyses can also be conducted for existing facilities, systems, subsystems, and equipment. Hazard tracking and risk resolution is initiated as soon as hazards and their associated risks have been identified. This effort is continued until the risk controls are successfully validated and verified. Accident and Incident investigation, as well as data collection and analysis are conducted throughout the life cycle, to identify other hazards or risks that affect the system. The specific details within this safety analysis process are further discussed in Chapter 4.

2.2.2 OSA and Comparative Safety Assessment (CSA)

The OSA and Comparative Safety Assessments are activities that occur prior to the establishment of baseline requirements. The OSA provides the system designers and management with a set of safety goals for design. It provides an environment description and a Preliminary Hazard List (PHL) for a given proposal or design change. The OSA assesses the potential severity of the hazards listed in the PHL. These severity codes are then mapped to a preset level of probabilities, which establishes the target safety level for controlling the hazard. For instance, a catastrophic hazard would be mapped to a probability requirement that is more stringent than a minor hazard. This process establishes the safety target level for controlling the hazard. This target level, or goal assists in the establishment of safety requirements for the system design.

The Comparative Safety Assessment (CSA) is an analysis type that provides management with a listing of all the hazards associated with a design change, along with a Comparative Safety Assessment for each alternative considered. It is used to rank the options for decision-making purposes. The CSA for a given proposal or design change uses the PHL developed for the OSA. The OSA process is depicted below in Figure 2-3.

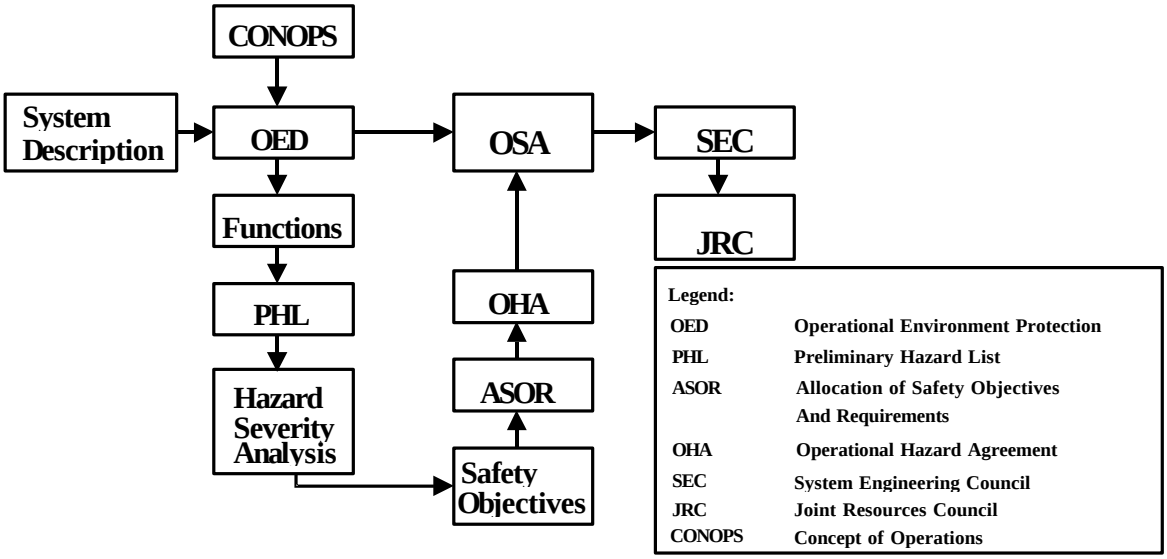

Figure 2-3: Operational Safety Assessment Process

2.2.3 Hazard Tracking and Risk Resolution

The purpose of hazard tracking and risk resolution is to ensure a closed loop process of identifying and controlling risks. A key part of this process, management risk acceptance, ensures that the management activity responsible for system development and fielding is aware of the hazards and makes a considered decision concerning the implementation of hazard controls. This process is shown in Figure 2-4.

Safety Action Record (SAR)

The SAR is used for tracking hazard records and contains the following:
Reference Number - This is a specific number assigned to a SAR.
Date - The date in which the SAR has been initiated.
Status - The status of the SAR is indicated as open, monitor, or closed.
Title - A specific appropriate short title of the SAR is indicated.
Description - The description defines the specific hazardous event under study and its worst case outcome. (The system safety related concern.)
Causes/Contributors - The contributory events singly or in combination that can create the event under study. Specific failures, malfunctions, anomalies, errors are indicated.
Risk (Severity and Likelihood) - The risk associated with the event is indicated. Initial risk (the risk prior to mitigation) is indicated. The residual risk (the worst case risks after the controls are implemented) is also indicated.
Suggested/Possible Mitigations/Controls - The design and/or administrative controls, precautions, and recommendations, to reduce risk are indicated. An objective is to design out the risks.
Evaluation - The appropriate activities and entities involved in the evaluation of the specific event are indicated.
Implemented Mitigations/ Controls - The design and/or administrative controls, precautions, and recommendations that have been verified within the design are indicated.
Verification and Validation - The verification and validation to assure that system safety is adequately demonstrated are indicated. Risk controls (mitigation) must be formally verified as being implemented. Safety verification is accomplished by the following methods: inspection, analysis, demonstration and test. Validation is the determination as to the adequacy of the control.
Narrative History - Provide a chronological living history of all of the actions taken relative to the SAR.
References - Appropriate references associated with the specific SAR are indicated, Analysis, Configuration Items, Software Units, Procedures, Tests, and Documents.
Originator(s) - The person(s) originating the SAR are listed.
Concurrence - Appropriate concurrence is required to status a SAR as closed (or monitor). IPT/ Program Management concurrence is required for residual risk acceptance. Other concurrence rationale is also documented, such as IPT (or FAA entity) concurrence.

2.2.4 Other Specific Safety Risk Management Processes

There are a number of other safety risk management processes discussed within the handbook involving commercial space and facility system safety. These processes are discussed within their specific chapters. This handbook does not discuss specific federal requirements associated with aircraft and ground certification processes. Consult the appropriate Federal Aviation Regulations for certification related processes.

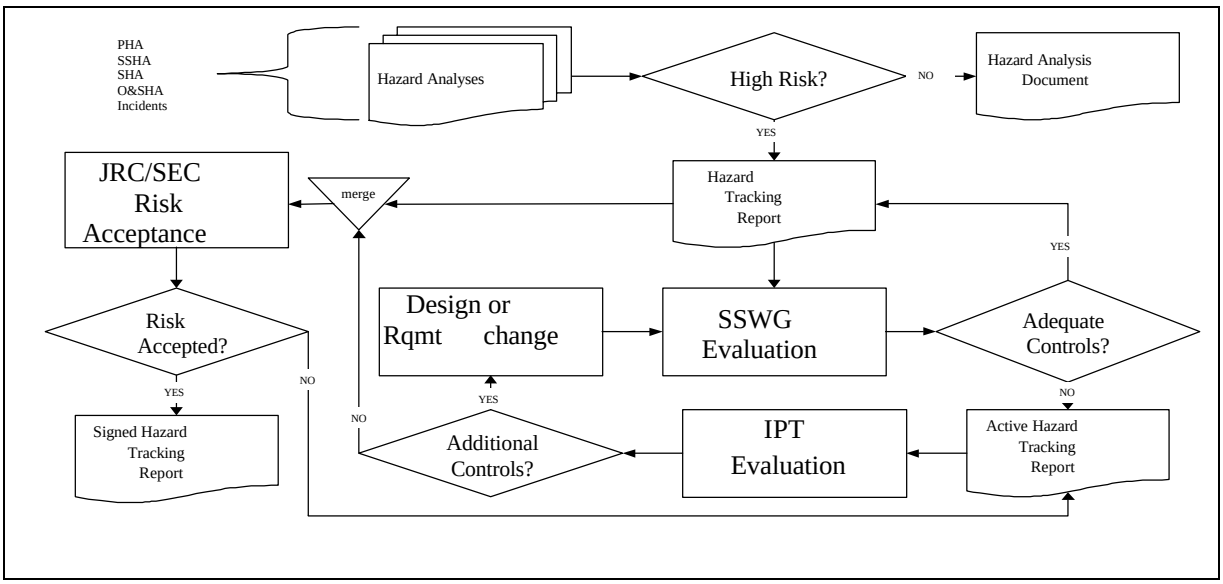

Figure 2-4: Hazard Tracking and Risk Resolution Process

2.2.5 FAA Corporate Comparative Safety Assessment Guidelines

FAA Report No. WP-59-FA7N1-97-2, Comparative Safety Assessment Guidelines for the Investment Analysis Process, Update of July 1999, presents guidelines for conducting life-cycle Comparative Safety Assessment as part of the FAA's Investment Analysis Process (IAP). Since the first publication of these Guidelines in June, 1997, information security, human factors and safety issues have gained viability and prominence as additional risks to be considered. Risk in this context relates to the "probability that an alternative under consideration in the IAP will fail to deliver the benefits projected for that alternative, either in whole or in part, and the consequences of this failure."